Pervasive Computing Goes the Last Hundred Feet with RFID Systems

Vince Stanford

EDITOR'S INTRODUCTION

Previously, I have discussed pervasive computing's business benefits and applications that pay their own way. These applications transport the enterprise database's benefits the "last hundred feet" directly to the point of work, sale, or service. Many are PDA-based, offering point-of-service terminals in clinical medicine, package delivery, and even restaurant ordering.

In this issue, I examine a different class of pervasive computers: Radio Frequency Identification tags. RFID tags turn everyday objects into network nodes that uplink IDs and status data to enterprise databases, storing new information as needed. They literally vanish into commonplace objects such as library books, shipping containers, car keys, luggage tags, clothing, or even pets, offering efficiencies in handling, location, and condition tracking. However, some people caution that we must implement privacy and security features from the ground up to avoid covert reuse of the tags. —*Vince Stanford*

What if networked computers were as cheap as paper clips and could be attached to things as easily as a yellow sticky? We are about to find out, because such computers are being deployed across the world as you read this. They are, of course, Radio Frequency Identification tags—low-power, short-range communication devices that we can embed into everyday objects to track location, monitor security, and record the status of events or even environmental conditions. Conceptualizing them simply as ID tags greatly underestimates their capabilities, considering some have local computing power, persistent storage, and communication capabilities.

RFID APPLICATIONS

This industry is very active, with numerous companies developing RFID tags of varying capabilities (see the "RFID Resources and Companies" sidebar). Broadly speaking, the RFID market is segmented into low-end and high-end tags. Low-end passive tags have approximately 32 bytes of local storage and are powered by the RF field generated by the readers. High-end tags can have full-blown microcontrollers and multiple interfaces to the environment, with local batteries to power them.

People often think of RFID tags as simply an updated replacement for the familiar bar code, but they differ in several important ways. Specifically, they

- Do not need line-of-sight access to be read
- Can be read simultaneously when many are present
- Carry more data, letting us identify individual items
- Can store new data from readers
- Can interface with environmental sensors and digital data sources

Make no mistake about it—at the high end, RFID tags are wireless, networked, pervasive computers, successfully integrated into their environment. They are easily attached, often of negligible weight and bulk, and offer many benefits for business, manufacturing, and tracking processes. Applications also exist at the retail level for individual consumers and shoppers, with many already deployed in real-world systems.

These systems' benefits are best understood in a full-system context, because isolated tags—such as scanners at the doors of retail stores—have limited uses until they connect to enterprise databases. Some currently used applications include

- *Access control*: RFID tags embedded into personal ID cards.
- *Baggage ID*: Passive tags embedded in paper luggage tags.
- *Automotive systems*: Keyless entry and immobilization systems.
- *Document tracking*: Passive tags affixed to documents.
- *Express-parcel tracking*: FedEx tags drivers and packages for various purposes.
- *Library checkout and check-in*: Passive tags in books.

1536-1268/03/$17.00 © 2003 IEEE ■ *Published by the IEEE CS and IEEE ComSoc*

APPLICATIONS

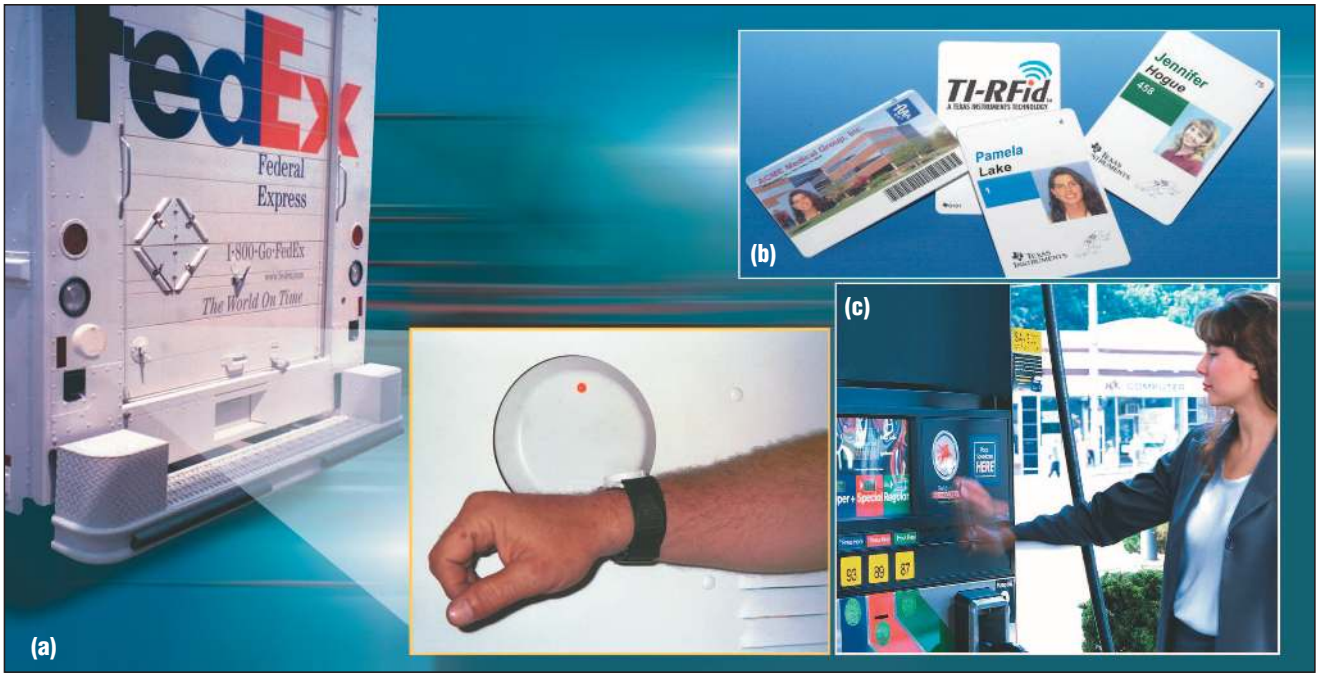

Figure 1. Existing RFID tag applications: (a) keyless entry for a FedEx driver; (b) personal identification badges; and (c) a Speedpass used for gasoline purchases. (photos courtesy of Texas Instruments)

- *Livestock or pet tracking*: Tags injected into pets, aiding recovery when they are lost.
- *Logistics and supply chain*: Container and product tracking.
- *Wireless commerce*: Speedpass and E-ZPass pay tolls and gasoline purchases.

Figure 1 illustrates three examples.

Furthermore, there are many areas in which we have not yet capitalized on RFID capabilities. One example includes recalling tainted food or medicine lots, perhaps even blocking them from sale in the first place using the point-of-sale terminals used in most stores. This is because even low-end RFID tags can identify the individual item or lot on which it is installed—and not just classes. Also, they can record the status of objects to which they are attached in important ways. For example, if a tagged hospital patient has received the morning dose of antibiotic, the tag could later upload the information to the clinical documentation system. RFID tags can monitor tamper seals, thermometers, or accelerometers to audit heat, shock, and vibration levels encountered by products in transit. They can also log accesses to shipping containers.

RFID RESOURCES AND COMPANIES

A large and vibrant RFID industry exists, offering Web sites that document, explain, and sell related product lines. The following list is only representative (space does not permit a comprehensive listing):

- Alien Technology (www.alientechnology.com) is developing self-assembly techniques that promise to drive the cost per tag to a few cents.
- Phillips Semiconductors (www.philips.com) offers a fairly extensive Web site describing its I-Code product line.
- *RFID Journal* (www.rfidjournal.com) contains numerous articles on RFID technology. You can obtain premium reports for a price, but a lot of useful material is free.
- Texas Instruments (www.ti.com) has lines of RFID tag and reader technologies, at both low-frequency (134.2 kHz) and mid- frequency (13.56 MHz) ranges. Its Web site is a particularly comprehensive resource with white papers, design notes, press releases, detailed product descriptions, and even an image library.
- Radio-Frequency-Identification (www.rfid-handbook.com) provides a useful, and free, overview of a book by the same name. There are editions in German, English, Chinese, and Japanese.

RFID MARKET SEGMENTS

Passive tags, often used for retail theft control or library checkout desks, receive power through inductive coupling of low-frequency broadcasts by readers. These can have indefinitely long life cycles because they do not require batteries to maintain the wake-and-query cycle that

THE ISO 15693 STANDARD FOR INTEROPERABLE RFID TAGS

Appropriate standards allowing numerous companies to create interoperable products are a key prerequisite to widespread use of RFID tags. ISO 15693, accepted in 2000, is one such standard (see www.iso.org). It is titled "Identification Cards—Contactless Integrated Circuit(s) Cards—Vicinity Cards" and has three parts: physical characteristics, air interface and initialization, and anticollision and transmission protocol. It specifies a 13.56-MHz RFID protocol, originally proposed by Texas Instruments and Philips Semiconductors in 1998, defining data exchange between RF tags and readers, and collision mediation when multiple tags are in a reader's RF field. Compliance guarantees that RF tags and readers using the ISO 15693-2 protocol will be compatible across companies and geographies. These are typically passive tags powered only by the reader's RF field, making them easy to manufacture and free of battery life limitations.

active tags use. However, they cannot observe their environment independently of a reader's power broadcast field.

High-end active tags, on the other hand, are usually battery powered and have a greater range than passive tags because they are not limited to reflecting the energy from the reader, with an inverse fourth-power signal diminution as a function of distance.

Passive tags

Early passive RFID tags were limited to simple fixed replies to an interrogating reader through reflected energy from resonant circuits. However, even passive RFID tags now have limited onboard read/write memory.

Figure 2 shows a variety of Texas Instruments passive mid-frequency, 13.56-MHz tags, with a 256-bit read/write memory organized into eight 32-bit blocks. These tags are programmable and can be locked to protect data from further modification. Additionally, they have data transmission rates in the range of 9 to 27 kBd, depending on the security and error detection and correction protocols used. This class of tags, represented by the TI TagIt and Philips I-Code tags, are designed to be compliant with the ISO-15693 RFID tag standard (see the related sidebar).

Active tags

I spoke with Peder Martin Evjen, Director of Technical Support at Chipcon, a company specializing in low-power RF devices headquartered in Oslo, Norway. The Chipcon RF tag line focuses on active tags that have high-end onboard capabilities and can integrate analog and digital interfaces to the outside world. These go well beyond the basic functions of passive tags, moving into functions of small wireless networked nodes. Furthermore, they have greater computing capability in an onboard 8051 8-bit microcontroller than first-generation desktop personal computers did in the early 1980's.

The Chipcon CC1010 can be read and written from distances in excess of 100 meters. This lets companies use them in loading docks to track the location of trucks, or on large cargo ships with many containers, which Evjen said is a major application (see the "US Customs Service Container Security Initiative" sidebar). Figure 3 shows a CC1010 tag and a tag programmer, used to download application programs.

Chipcon can integrate the CC1010 tag with analog sensors and digital data sources, because it supports three ADC (analog-to-digital converter) channels, a Universal Asynchronous Receiver Transmitter (UART), and several general I/O pins. These let the tag monitor sensors that are placed, for example, on or in shipping containers as required by the Container Security Initiative (see the related sidebar). Chipcon designed the CC1010 line mainly for frequency-shift keying systems in the ISM/SRD (Industrial, Scientific, and Medical/short-range devices) bands at 315, 433, 868, and 915 MHz, but it can program the line to frequencies between 300 and 1,000 MHz. These interfaces let the tags monitor sensors such as accelerometers and thermometers that can record temperature, shock, and vibration levels. Also, Chipcon can digitize internal sensors to record conditions inside containers to indicate if potentially toxic volatiles have leaked from the individual packaging.

Chipcon can also equip the CC1010 tag with an 8051 microcontroller to manage 32K nonvolatile flash memory containing programs and data, and 2K of static RAM for scratch purposes.

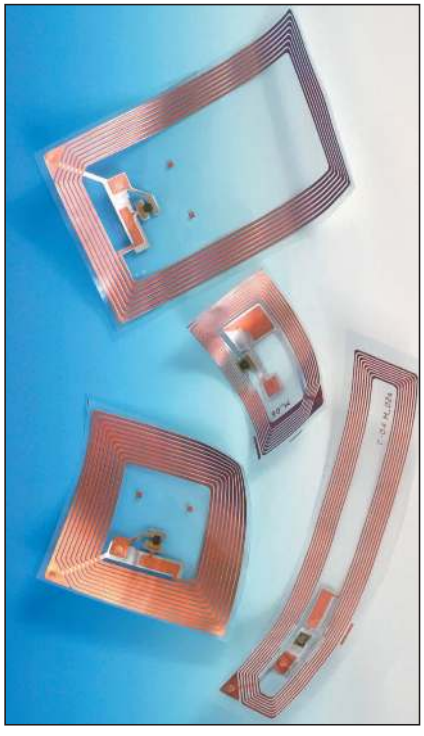

Figure 2. Texas Instruments TagIt passive RFID tags have onboard read/write memories. These tags are delivered in a polymer substrate in reels for easy handling. They are so cheap that they are disposable and truly pervasive. (photo courtesy of Texas Instruments)

APPLICATIONS

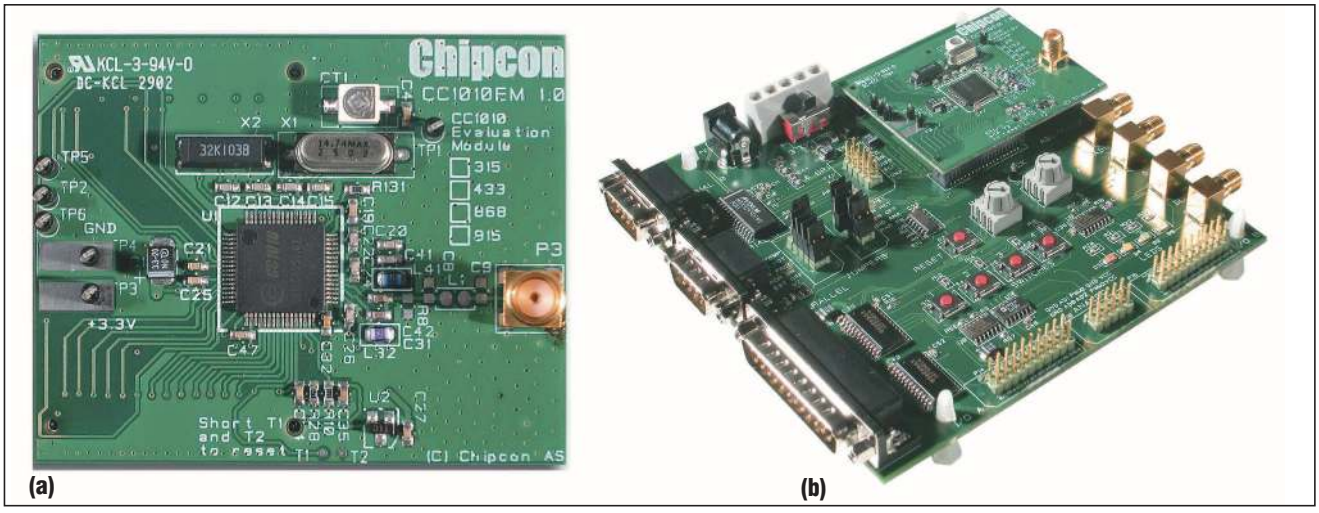

Figure 3. (a) A Chipcon CC1010 tag with (b) a programmer board. Like all embedded computers, these come with software and hardware development tools. (photo courtesy of Chipcon)

Onboard, the tag supports a serial peripheral interface, and for encryption, a hardware Data Encryption Standard chip for secure communication. The 32K flash RAM is divided into 256 pages with programmable protection flags that can prevent unauthorized downloading of internal programs and data, such as encryption keys and sensor monitor routines already loaded into the tags. The tag can reload software from a reader through a duplex RF link using an RF boot loader, provided that the previous version is erased before reprogramming. This prevents malicious downloading and reprogramming with modified data and code, which could circumvent the security functions the tags are designed to provide.

In very large quantities, these high-end tags cost less than US$4 each, so deployment to protect high-value cargos that are subject to environmental hazards makes economic sense. These tags' battery life lets them operate for months, or even years, with a typical life cycle including many trips on reusable shipping containers before they are replaced.

Chipcon tags can be programmed in a variant of C with its own development tools such as an integrated development environment and a debugger. These tools allow cross-development on PCs for the microcontroller-based RFID tags. There is also a library of example programs that can serve as design patterns. Additionally, the development tools can run an open operating system called Tiny OS designed for processing real-time event-

US CUSTOMS SERVICE CONTAINER SECURITY INITIATIVE

According to the US Coast Guard in its December 2002 report *Maritime Strategy for Homeland Security* (see www.uscg.mil), the maritime transportation system handles more than 2 billion tons of freight, 3 billion tons of oil, 134 million ferry passengers, and 7 million cruise ship passengers. On the order of 7,500 ships, manned by 200,000 sailors, enter US ports annually to off-load approximately 6 million truck-size cargo containers onto US docks.

To deal with security threats posed by this volume of container shipping, the US Customs Service (www.customs.gov) is proposing the Container Security Initiative to identify high-risk containers and secure them with tamper-detection systems. The initiative aims to expedite processing of containers prescreened at points of embarkation in overseas megaports participating in the initiative. The CSI's basic goal is to first engage the ports that send the highest volumes of container traffic into the US, as well as the governments in these locations, in a way that will facilitate detection of potential problems at the earliest possible time.

To meet this requirement, high-end RFID tags could periodically monitor electronic seals on the containers during transit. This class of application requires tags that can integrate sensor management electronics, such as analog-to-digital converters, and digital data interfaces. Tampering can also be detected in real time, and the tags, as the lowest level of a multitier architecture, can relay data to alert the shippers or customs authorities of tampering as it occurs.

Similarly, Chipcon tags are used extensively to transport high-value goods in the US as well as worldwide. There is also great potential in Europe. For example, Norway is a major exporter of salmon, so the RFID tags record the temperature in the containers so that the buyer can verify product freshness. This can be especially important when the shipments are bound for southern locations such as Italy, Spain, or North Africa.

driven programs in embedded systems (see http://today.cs.berkeley.edu/tos). The system provides a component-based abstract hardware model, RF messaging protocols, periodic timer events, asynchronous access to UART data transfer, and mechanisms for persistent storage.

WHITHER PRIVACY?

As the cost of RFID tags drops from several dollars to several cents, the tags will almost certainly appear in an increasing variety of retail items. The MIT Auto-ID Center (www.autoidcenter.org) presents a heady vision: "By creating an open global network that can identify anything, anywhere, automatically, [the Auto-ID Center] seeks to give companies something that, until now, they have only dreamed of: near-perfect supply chain visibility." This will be based on RFID tags of negligible individual cost, and the efficiencies made possible by the tags in the supply chain are absolutely compelling to businesses. However, unless these systems are properly architected, they can cause massive collateral damage to consumer privacy.

A cautionary story for retail merchants emerged when it was widely reported that Italian clothing retailer Benetton planned to deploy RFID tags for some clothing lines. There was no mention in the press releases of the tag supplier, Philips Electronics, on how to disable the tags after the sale. There was a massive consumer reaction, which the press came to refer to as the Benetton Brouhaha. Because the modern passive RFID tag carries enough data bits to identify the individual garment and not just its type, consumers were concerned that the garments would be associated with the purchaser at the point of sale and added to a database. Then the tags would radiate identifying information to any tag reader anywhere, tracking their every movement.

Consumers and privacy groups are also concerned that live RFID tags in clothing, automobile tires, and food items will allow undue surveillance opportunities. This concern came to a boil when consumers called for a boycott against Benetton. The public outcry generated by the deployment of an RFID tag system without proper privacy architecture caused Benetton to withdraw from actually deploying the RFID system.

ARCHITECTURES FOR ETHICAL PERVASIVE COMPUTING

I spoke with the MIT Laboratory for Computer Science's longtime privacy advocate, Simson Garfinkel, author of *Practical UNIX and Internet Security* and several other books on network security and privacy. (See the "Privacy Resources for a Pervasively Networked World" sidebar for more information.) He has also recently authored a white paper titled *Adopting Fair Information Practices to Low Cost RFID Systems*, which discusses approaches to ensure

APPLICATIONS

PRIVACY RESOURCES

MIT's Simson Garfinkel is a well-known writer on privacy, network, and system security—and, of course, personal encryption technology. According to Garfinkel, we can preserve privacy in a networked world if we care enough to do so. After all, privacy in a networked world begins with our understanding and securing our own systems and networks. This will only become more important in the pervasive future, but system architects and designers will have to make this a part of the design goals, and citizens will have to insist that this be done.

A few of Garfinkel's books (O'Reilly and Associates) include

- *Database Nation: The Death of Privacy in the 21st Century*
- *PGP: Pretty Good Privacy*
- *Practical Unix and Internet Security: 3rd Edition*, with Gene Spafford and Alan Schwartz
- *Web Security, Privacy, and Commerce*, with Gene Spafford

Other resources on privacy include

- CASPIAN (www.nocards.org), a Web site initially devoted to discussing electronic tracking systems including customer cards in grocery stores, but lately covering RFID tags as well
- Electronic Frontier Foundation (www.eff.org), a well-known and broad Web site on citizens' rights in the digital millennium
- Privacy Rights Clearing House (www.privacyrights.org), a Web site on privacy in the electronic age, with resources and links to many others

personal privacy and technologies to prevent abuse of the tags (available at www.simson.net). The white paper also discusses how people can abuse this technology by using covert tag readers to track items that are associated with individuals.

Garfinkel said the Benetton Brouhaha did not surprise him, because both Benetton and Philips Electronics "utterly ignored" privacy protocols that could have password-protected or even erased the tags' data. He further said that Benetton could have avoided the problems by using such password-protection tags, prohibiting promiscuous responses to tag readers.

Furthermore, he pointed out that consumers are not the only stakeholders with an interest in privacy protocols. For example, large retailers, such as Wal-Mart, would not want a competitor to be able to walk the aisles of a store with a reader in his or her pocket and covertly accumulate a complete inventory that could be used for purposes disadvantageous to its inadvertent provider. This would allow industrial espionage on an unprecedented scale.

When asked the ranges at which passive tags can be read, Garfinkel said that the physics of passive tags will always be limited by the inverse fourth-power law, because reader field strength declines at an inverse square and the reflected energy return also declines at an inverse square. However, readers can be placed almost anywhere people move and work, and with tags that respond promiscuously to any reader, it is a virtual certainty that they will be abused. Moreover, privacy architectures must be predicated on the sure knowledge that the tags and readers are rapidly declining to price levels approaching zero and will be truly pervasive in the environment. We are entering at the threshold of a world in which you *will* be read if your RFID tags respond to queries.

Another example Garfinkel gave was the electronic toll-collection system in Massachusetts, originally deployed to collect tolls using an account-based system rather that an anonymous digital cash system. The electronic toll-collection system tags are actually hybrid tags rather than passive ones and have a battery that can boost the return signal's strength and thus can be read at substantial distances. Moreover, uses of these tags are experiencing scope creep, with traffic management systems now using electronic toll-collection system tags to sense traffic volumes. Some states are already using these passes to compute speed and issue automatic traffic tickets. While several digital-cash systems avoid this kind of wholesale disclosure of personal information, the electronic toll-collection system in Massachusetts did not use them. Systems with profound social consequences are being deployed routinely with little concern for or understanding of their impact on individual privacy.

The market for RFID tags is already well established, and the near future will see the emergence of even more capable active tags that can be integrated into nearly everything we wish to track. They will offer new economies through the supply chain, allow greater security to retail establishments, and provide easier ways to process payments. As a caution, however, experience to date suggests that we must design these systems with features that preserve privacy. Otherwise, they could be used in many ways that are not in the interest of people who carry them. Those used for financial transactions, for example, should be designed to allow the end user to control whether, and how, tags will respond to queries. P

Vince Stanford is the lead engineer for the NIST Smart Space Laboratory, project manager for the NIST Smart Space project, and a founding member of *IEEE Pervasive Computing* magazine. He writes here as a volunteer; NIST does not endorse any opinions or information presented in the magazine. Contact him at vince-stanford@users.sourceforge.net.