NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTER
A program of the National Institute of Justice

From Summer 2005 *TechBeat*

TECH b•e•a•t

Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences

Technology Primer: Radio Frequency Identification

An inmate's daily movements are tracked and monitored, and a record of each movement is automatically stored in a central database. An unauthorized person removes a piece of evidence from its secure location in the evidence control room; at once, an alert notification goes out to a central monitoring station. Terrorists tamper with a shipping container, but scanning the container reveals the tampering before it is allowed into a U.S. port.

These are a few of the current and potential applications in corrections, homeland security, and law enforcement for radio frequency identification (RFID), a wireless communications technology that enables users to authenticate, locate, and track objects or people tagged with a unique identifier.

RFID technology traces its beginnings to World War II, when it was used to identify aircraft. However, it has become commercially viable only in the past two decades as a result of advances in radio frequency electronics, information technology, and materials science.

How RFID Works

An RFID system has three basic components: tags, readers, and a host computer. RFID tags contain tiny semiconductor chips and miniaturized antennas inside some form of packaging. Some RFID tags look like paper labels and are applied to boxes and packaging. Others are incorporated into the walls of injection-molded plastic containers. Still others are built into wristbands. Each tag is programmed with a unique identifier that allows wireless tracking of the object or person the tag is fastened to. Because the chips used in RFID tags can hold a large amount of data, they can also include such information as serial numbers, time stamps, configuration instructions, technical data, medical records, and travel history.

Like broadcast television and radio, RFID systems use four major frequency bands: low frequency (LF), high frequency (HF), ultrahigh frequency (UHF), or microwave. Systems coming on the market today operate in the UHF band, whereas older RFID systems typically use the LF and HF bands. The microwave band is being reserved for future applications.

RFID tags may be powered by a miniature battery inside the tag (active tags) or by an RFID reader that "wakes up" the tag to request a reply when the tag comes within range (passive tags). Active RFID tags may be read up to 100 feet from the RFID reader and may be either "smart" tags (with memories that can be written to and erased like a computer hard disk) or read-only tags. Passive RFID tags can be read from up to about 20 feet away and generally have read-only memory. Tag size and cost, read range, read/write accuracy, data rate, and system functionality vary according to which features are included in the design and which frequency band the RFID system uses.

RFID readers are composed of an antenna that communicates with the RFID tags and an electronics module networked to the host computer. The module relays messages between the host computer and all the tags within the antenna's read range, enabling one reader to communicate with hundreds of tags simultaneously. It also performs security functions such as encryption/decryption and user authentication. RFID readers can detect tags even with no clear line of sight between them.

Most RFID networks are composed of many tags and many readers networked together by a central host computer, most often a desktop workstation. The host processes the data the readers collect from the tags and shuttles it between the RFID network and larger enterprise information technology (IT) systems, where supply chain management or asset management databases may operate. "Middleware," software that connects the RFID system with an IT system, manages the data flow.

Current RFID Applications

Commercial applications for inventory and supply chain management are driving the development and growth of RFID technology. Wal-Mart®, the world's largest retailer, and the U.S. Department of Defense (DoD), the

world's largest supply chain operator, have spurred this growth by requiring suppliers to use RFID tags. Wal-Mart required its top 100 suppliers to begin tagging pallets and cases with passive RFID tags by January 1, 2005, prompting other retailers to announce similar plans. DoD quickly followed suit, and additionally requires containers shipped outside the continental United States to have active RFID tags that identify content and point of origin.

Wal-Mart's and DoD's size and RFID mandates have helped bring this technology into the mainstream and make it more cost effective. Their specifications have also spurred the RFID industry to unite behind a single technology standard, EPCglobal's Electronic Product Code™ (EPC).

The drive to incorporate RFID technology into supply chains is motivated by the advantages that pallet-level visibility of inventory offers: increased shipping, receiving, and stocking efficiency and decreased costs for labor, storage, and inventory loss. RFID readers installed at loading dock doors can detect RFID tags on merchandise or pallets passing through the doors. The reader sends a command to the tags to transmit their identities, collects this information, and forwards it to the host computer. The host then credits or debits the inventory database depending on whether the merchandise is coming or going. If the system uses smart tags, the host computer can write the shipping/receiving date and time onto the tags.

The same capabilities that make RFID ideal for managing supply chains give it great potential for corrections, homeland security, and law enforcement. Applications include property tracking (e.g., firearms, communications equipment, computers), evidence tracking, passport and visa tracking, tracking inmates and staff within corrections facilities, and access control systems for buildings and rooms (e.g., keyless entry devices). RFID technology has made greater inroads in corrections and homeland security than in law enforcement.

RFID in Corrections

RFID technology enables correctional facilities to convert routine manual tasks that require costly staff time to electronic functions performed automatically at a minimal cost. In addition to promoting operational savings and creating a more effective and efficient correctional system, the use of RFID systems helps increase security, decrease violence, and create a safer environment for inmates and staff.

Correctional facilities in California, Michigan, Illinois, and Ohio are already using an RFID tracking system developed by an Arizona-based company. This system has five primary components: a tamper-detecting wristwatch-sized transmitter for inmates, a belt-mounted transmitter worn by officers, a strategically placed array of receiving antennae, a computer system, and proprietary application software.

The transmitters worn by inmates and officers send unique radio signals every 2 seconds, enabling the system to pinpoint the wearer's location and track and record his or her movements about the facility in real time. In effect, the system automatically conducts an electronic head count every 2 seconds and sends an alarm if an inmate is missing. If an inmate enters a restricted area or attempts to remove the wristband transmitter, the device signals an alarm to the monitoring computer. If an inmate knocks an officer down or removes the transmitter from the officer's belt, the officer's transmitter sends an alarm. Officers can also send an alarm by pressing an emergency button on the transmitter.

The RFID system records all tracking data collected over a prescribed period in a permanently archived database. This enables the system to identify and report all inmates in the vicinity of any incident that triggers an alarm. Other management reporting applications include medicine and meal distribution, adherence to time schedules, and specific arrival and departure information.

RFID in Homeland Security

The U.S. Department of Homeland Security (DHS) has embraced RFID as a technology of choice for improving security at U.S. borders and ports of entry. RFID technology is ideal for locating, tracking, and authenticating the movements of people and objects as they enter and depart the United States.

In January 2005, DHS announced plans to begin testing RFID technology under its US–VISIT initiative, which now uses biometric technology to verify the identity of foreign visitors at 115 airports and 14 seaports. A visitor's index fingers are scanned to obtain digital fingerprints and a digital photograph is taken. The fingerprints and photograph are used to authenticate the visitor's travel documents and are recorded and checked against terrorist watch lists.

To automate the entry-exit process, the DHS proof-of-concept test will assign visitors entering the country an RFID tag with a unique serial ID number that links to their digital fingerprints, photos, and other personal information in US–VISIT's secure database. The initiative will use passive read-only tags that cannot be altered. No personal information will be stored on the tag.

RFID technology is expected to improve the ability of U.S. Customs and Border Protection officers to match entries to exits at land borders rapidly, accurately, and reliably. RFID tags will permit automatic recording of arrivals and departures of visitors in pedestrian and vehicle lanes and could give border personnel quick verification on the length of a visitor's stay in the United

States and whether he or she overextended a visa. RFID testing is scheduled to begin at the ports of Nogales East and Nogales West in Arizona, Alexandria Bay in New York, and Pacific Highway and Peace Arch in the State of Washington by July 2005. Testing will continue through spring 2006.

Preventing weapons of mass destruction from entering the United States via cargo containers is another top priority for DHS. Under the Container Security Initiative (CSI), announced in 2002, gamma or X-ray imaging and radiation detection equipment is being used to examine cargo containers before they are shipped to the United States. CSI also calls for the development of "smart" tamper-evident containers—a clear-cut application for RFID technology. Certainly, RFID will be a key component in the Nation's efforts to secure its borders and transportation systems.

RFID in Law Enforcement

Law enforcement agencies have shown less interest in RFID technology than corrections and homeland security agencies, in part because of privacy concerns that will be discussed later. However, some RFID applications that will benefit law enforcement simply require the collaboration of other areas of government or of commercial manufacturers. RFID law enforcement applications fall into three main categories: evidence handling and property control, crimefighting, and officer safety.

RFID systems may prove more effective and efficient than barcodes for recording, locating, and tracking evidence and property. RFID smart tags are ideally suited to meeting chain-of-custody requirements. These tags can record the who, what, where, and when of each piece of evidence from a crime scene and, once the evidence is stored in a secure location, send an alarm automatically if anyone attempts to tamper with it. They can also track and record such valuable police equipment as firearms and laptop computers. RFID technology also enables the assignment of a particular piece of equipment to a specific officer.

As consumer-goods manufacturers adopt RFID tagging, the technology's tracking and tracing capabilities will help law enforcement identify and recover stolen merchandise and provide evidence in court. RFID tagging will also help prevent counterfeiting because the tags are difficult to forge or copy. Incorporating unobtrusive RFID tags into consumer goods will make it easy to tell the real thing from a knockoff.

An initiative to use RFID technology to reduce property crime, called "Chipping of Goods," is underway in the United Kingdom. In the future, any RFID-enabled object found at a crime scene, from an empty soda can to a knife, conceivably could be traced through the supply chain to a retailer. If the object was purchased with a credit card or a customer loyalty card, it could be traced back to the purchaser, giving the police the identity of a potential suspect or witness to the crime.

Applying RFID technology to license plates has the potential to help law enforcement in a variety of ways, from tracking stolen vehicles or vehicles used in the commission of a crime to enforcing speed limits. A U.K. company is developing a system that will allow a network of fixed and portable RFID readers to identify tags embedded in license plates up to 300 feet away. The tag will send a unique identifier to a central system that will use it to access data such as the vehicle registration number, make, model, and color, and the owner's name, address, and other information.

A more controversial proposed use of RFID's tracking capabilities in law enforcement has been the promotion of officer safety by tracking officers' locations throughout their shifts. The police union in Orlando, Florida, resisted the department's attempt to conduct a pilot test of a system designed for this purpose that combined RFID and global positioning system technology. The union held that continuous monitoring of an officer in day-to-day police work was intrusive. The department canceled the project.

Privacy Issues

The same features that make RFID a valuable technology for corrections, homeland security, and law enforcement also raise serious concerns about privacy that may limit its use. Consumer privacy and civil liberties organizations have pointed out that, if used improperly, the ability to identify, locate, track, and monitor people and objects with hidden tag readers jeopardizes individual privacy, reduces or eliminates consumer anonymity, and threatens civil liberties.

As mentioned earlier, police officers in Orlando, Florida, found an RFID tracking system intended to ensure officer safety to be too intrusive, and union resistance to the project closed it down. Corrections will likely confront even thornier issues now that the U.S. Food and Drug Administration has approved an RFID chip that can be implanted in humans. The possibility of replacing devices worn on inmates' wrists with subdermal microchips that are less subject to tampering but considerably more invasive raises serious social and ethical issues.

The availability of RFID applications with the potential to help law enforcement fight crime and increase national security raises the stakes in the debate between RFID proponents and privacy advocates. In October 2004, the Commonwealth of Virginia held hearings to explore creating an RFID-enabled driver's license that eventually would include biometric data such as fingerprints or retinal scans. Such a license could not easily be forged, would

be nearly impossible to use for identification if stolen, and would streamline checking of licenses by law enforcement and other government officials. However, an RFID license would also allow authorities to profile and track citizens nationwide without their knowledge or consent, because RFID tags can be read from a distance and RFID readers can easily be hidden. Privacy advocates also noted during the Virginia hearings that an RFID driver's license could lead to the development of a national identification system without actually creating a national ID card.

Several States have introduced legislation to set limits on the use of RFID technology. A congressional subcommittee has also held hearings on RFID technology, and the Federal Trade Commission has convened a workshop to determine if Federal regulation is necessary.

On the Horizon

Significant growth in the use of RFID technology is expected over the next 5 years. Proponents of the technology predict that RFID tags will someday be as pervasive as barcodes. Corrections, homeland security, and law enforcement have much to gain from the continued development, testing, evaluation, and demonstration of RFID tools. Being proactive offers each field the best opportunity to have a hand in shaping these tools to best serve its unique needs.

For more information about radio frequency identification technology, the following websites are a good place to begin: www.rfidjournal.com, www.rfidnews.org, and www.rfid-101.com.

This article was reprinted from the Summer 2005 edition of *TechBeat,* the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center system, a program of the National Institute of Justice under Cooperative Agreement #96–MU–MU–K011, awarded by the U.S. Department of Justice.