

Companies, Agencies Use Clandestine RFID Systems to Catch Thieves

The NOX system includes RFID readers embedded in walls, surveillance cameras and—in some cases—luminescent dust to track the movement of personnel and assets.

By Claire Swedberg

March 20, 2008—A handful of government agencies and private companies such as electronics suppliers are employing a clandestine RFID system known as NOX that allows them to use RFID interrogators hidden in walls, in conjunction with video surveillance and, in some cases, luminescent dust, to thwart theft or other unauthorized activities within their facilities.

The NOX system is the creation of [SimplyRFID](#), a company based in Warrenton, Va. Founded in 2002 by its president, Carl Brown, SimplyRFID has developed RFID solutions for a number of clients, including [Stamps.com](#), [UPS](#), [FedEx](#), the [U.S. Postal Service](#) and [Target](#), and its Pro-Tags product line is aimed at suppliers to the [U.S. Department of Defense](#) (DOD). During the past few years, Brown says, the company has moved into the clandestine market, following government interest in the use of RFID to prevent theft, or to monitor the movements of personnel wearing RFID-tagged badges.

Because of its location near Washington, D.C., SimplyRFID attracted the attention of several government agencies, including the [FBI](#), which visited the company's office to purchase RFID readers and tags, but brought the hardware back to their location and installed the equipment themselves. "What we found was that they were happy to have any technology that would help them [with security]," Brown says. So the company began developing a more comprehensive security solution that included RFID with video surveillance and, in some cases, "optically charged" dust that could be tracked with cameras.

The NOX system uses RFID readers that can be embedded in walls, as well as surveillance cameras that can be hidden if so desired by a user. The system integrates the two functions to enable users to track theft or other undesirable behavior on their property. By linking RFID tracking with video footage, Brown says, users can not only know which items might be missing by tracking the locations of their assets, they can also link to video footage to determine what has occurred.

"The big problem in selling RFID is that it is not always a solution by itself," Brown states. Instead, he adds, RFID offers part of a security solution by helping users track activity without requiring them to watch it around the clock. But in conjunction with video surveillance, he says, users have information about activities that have occurred—such as which items were moved, as well as where and at what time—reinforced by a visual image of what transpired.

Brown likens RFID technology to a fence, which still has vulnerabilities. People can find ways around that fence, he explains, by not wearing their badge, by wearing someone else's badge or by tampering with an RFID sticker. Such vulnerabilities make video surveillance and optical dust a strong addition to RFID. The optically charged dust consists of microporous fibers that glow when exposed to low-power laser light. This

luminescence is not visible to the human eye but can be detected by a video camera. The dust is scattered in areas where there is a risk of unauthorized activity, or where entry is generally forbidden.

A camera can be programmed to watch for any dust that a person might inadvertently pick up by walking through an unauthorized area. When that individual passes in front of the camera, it detects the glow as the dust is illuminated by a laser and triggers an alarm. According to Brown, this system provides perimeter security from trespassers or wild animals that might enter a secured property.

Following interest from government agencies, SimplyRFID began providing its solution to the private sector, with clients (all of which wished to be unnamed for this article) located in such states as California, Texas and Florida. The systems allow them to track their employees, as well as high-value assets that, in many cases, pass through their facilities in large quantities and can end up missing.

One common practice for thieves, Brown says, is to load extra items—such as TVs or computers—onto a shipment, or to take assets to the recycling or trash area, where they can then be removed by another party. In some instances, these thefts can occur in extremely high volume, Brown says, adding that companies have had entire trailers loaded with assets disappear. Most firms, he notes, aren't interested in prosecuting, as much as in putting an end to the thievery. "They just want to find out who's doing it and stop it," he says.

By placing tags on assets, as well as on personnel badges and such items as garbage cans, companies can track what is moving, and where. The cameras, Brown says, record all activity in their area and are generally used for forensic purposes. If items are determined to have been shipped when they were not ordered, and if that occurred repeatedly with one specific employee, a company can view video footage at the time of the occurrences to see what happened.

Brown says SimplyRFID uses RFID interrogators from [Thing Magic](#) and [Motorola](#), among other vendors. A reader is typically installed in a wall at night, or during off-hours, and is connected via an Ethernet cable to a [Dell](#) computer server so the data can be reviewed by the company's security personnel.

Companies often install four or five clandestine readers, and about the same number of cameras, at sites where items have disappeared. In other cases, companies arm every doorway and dock door with an RFID interrogator and tag every item inside. Of the private customers for which NOX has been available since 2007, Brown says, "We have three in full deployment and nine others in pilot phases. We are adding about one new install per month."

The companies use the RFID readers to capture ID numbers and send that data to a Dell computer server capable of managing up to 100 interrogators. NOX software allows integration of RFID tag data and video imagery—also stored on the server—so that an image from the time and place of a specific RFID tag read can be automatically displayed on a computer screen, along with the name and ID numbers of the tagged assets and employees wearing RFID-enabled badges.

RELATED ARTICLES Most cameras are supplied by [Axis Communications](#), Brown says. The NOX system uses [Avery Dennison](#) EPC Gen 2 UHF tags.

The cost for a NOX deployment can be around \$40,000 for four or five readers, cameras and software. For larger deployments with more than 30 antennas and 15 cameras, Brown says, the cost averages \$100,000 to \$150,000. SimplyRFID also offers installation services, he adds, though users often do some of the work themselves, such as installing the cables connecting the interrogators, cameras and server. Other end users, including government agencies, prefer to handle installation entirely on their own.