Hal Berghel

RFID AND THE FINE ART OF NUANCE

"Nuance" is a 6-letter word; but Nuance isn't.

We're all going to take the pipe on this one. As it so often happens in technology, herd mentality displaces thoughtful reflection, and RFID is unfortunately thought of as an IT silver bullet for tracking. Nothing could be further from the truth.

A few years back I worked with a civil engineer who was a legend in his own mind. He discovered the web in the late 1990s, and after that he fashioned himself as an IT guru. One of his first decisions was to use electronics to enhance physical building security. Proudly he proclaimed, "You see, with proximity cards we will have a record of who accesses our facilities." I pointed out to him that what he really had was a record of what card was used to unlock the doors. I got one of those lights-on-but-nobody-is-home looks, and let the matter drop. The point is that engineers are great at some things - I know I wouldn't want to drive over a bridge that wasn't designed by a professional engineer - but they're weak at others. One of the things that they're weakest at is an appreciation of nuance. The reality check that I gave the civil engineer was in his mind a nuance. So it is with the deficiencies of RFID technology.

Let me illustrate. I first gained appreciation of GPS technology when I worked in Northwest Arkansas. My oldest son was a good friend of the grandson of J.B. Hunt (of trucking fame) and so I'd run in to J.B. at birthday parties, soccer games, and so forth.

J.B. loved to talk about trucking, and I am an active listener. Sometime in the early 1990s he told me of this new GPS technology that he was using to locate his 5,000 trucks in real time. I thought this was pretty nifty, so at the first opportunity I bought a GPS chart plotter for my boat, then a pocket version for hiking, and by the late 1990s GPS for my cars. I now buy Tom Tom's by the 6-pack and haven't read a map in years. I have become as dependent on GPS now as I became on pocket calculators in the 1970s. Unfortunately, only my GPS talks to me. (I've developed a very close bond with Eva, incidentally.).

So I'm comfortable with GPS. I understand how it works. But more importantly, I know its limitations. As long as the satellites are reliable, and the electronics are functioning correctly, a GPS unit can be relied upon to tell us where it is. Note: it cannot tell us where we are, unless we are where it is (this is a nuance!). More importantly, it cannot tell us what clothes we're wearing when we're near it (this is a second order nuance).

So the rest of the story is that during a discussion of GPS recently, a colleague informed me that there are services now that can tell us with certainty where a shipment is because GPS in transport vehicles are now linked to the manifest by RFID. Think back to my discussion of the civil engineer and the prox cards. As Yogi Berra said, this is deja vu all over again.

RFID Basics

RFID stands for Radio Frequency ID. The key term is "radio frequency." Think of RFID as a kind of WiFi for objects. Until someone can train radio frequencies to obey property lines, RF systems of any stripe join WiFi as magnets for vulnerabilities.

The idea behind RFID was to create what some have called an "Internet of Objects." A giant swarm of things that cry out "look at me, I'm S/N 9347201-349349872347 and my price is $4.53." What makes RFID particularly attractive is (1) it's cheap, (2) it's versatile, (3) it can be read at distance regardless of position and orientation, (4) it's fast. RFID is like a talking bar code with an electronic voice.

RFID technology is now ubiquitous - motivated by companies like Wal-Mart (whose company headquarters is just a few miles from J.B. Hunt's, incidentally) that have industrial-strength inventory control and supply chain challenges. The DoD was so impressed with Wal-Mart's RFID initiative in fact, that they mandated RFID use for DoD vendors in 2003. When a 3-letter government agency listens to a business, that business has stroke! Target and other retailers followed suit, followed closely by other industries and veterinarians. That's right, Bowser or Tweetums may have an RFID tag hidden where the sun don't shine. (If you've had any invasive medical procedures yourself, you might want to have yourself scanned. Just kidding. Or am I?)

In any case RFID involves a really small transponder embedded in a transport medium (e.g., a small piece of plastic), a tiny computer connected to the transponder, and some external readers. IBM was one of the first companies to get into the commercial RFID space. They were also one of the first companies to get out of the RFID space - they sold their equipment and patent rights to Intermec Technologies a few years ago. IBM transitioned into RFID early on since they were already into the "auto-ID" space with UPC bar code technology. (In one of life's little ironies, the inventors of the bar code tried to interest IBM in licensing the first bar code patent in 1952, but the whiz kid managers at IBM couldn't see the value. IBM then asked one of the inventors who by this time worked for IBM to reincarnate the bar code for UPC use in the mid 1970's).

The concept of RFID is pretty simple: the data is stored on a miniature transponder called an RFID chip or "tag." The communication with the transponder is accomplished with a reader which is connected to a host computer. The reader may be thought of as just a high-powered transponder itself. The tags may be active or passive depending on whether they have their own battery power. Passive tags derive their power from the RF signal from the reader. In the U.S., RFID transponders and readers usually operate on FCC licensed frequencies and power ranges, e.g., 902-928 MHz @ 4 watts. The trade-offs that are most relevant to our present discussion is that (a) the higher the frequency, the greater the effective distance between tag and reader, and (b) the active tags operate at greater distances than passive tags. Needless to say, there are tag/reader combinations that may be optimized for read speed, distance, accuracy, motion, climate, and so forth. Most RFID tags are write-once-read-many. Many of you already have RFID systems in place in your companies to mon-

itor everything from food and beverage to high-value chips, so you need no convincing that we can create a reliable RFID interrogation tunnel for highways and railroads.

The Nuance Returns

So this colleague informs me that there are services now that can tell us with certainty where a shipment is because GPS in transport vehicles are now linked to the manifest by RFID. We know that GPS works. We know that RFID works. And we know that since both are digital technologies, we can interface them with little effort. So what's the problem?

The problem is conceptual. GPS technology can establish the location of the GPS unit. RFID technology can recognize data in RF broadcasts between tags and readers. No problem there. But where does the manifest fit in the scheme of things? Well, it doesn't, strictly speaking, because it is an ancillary component of the system. The only way the manifest can be logically linked is if a verifiable association can be made between the manifest-of-record, the GPS coordinates, and the RFID data. In this case, the keyword is "verifiable."

Let's create a hypothetical scenario to illustrate the problem. Suppose company X orders a truckload of widgets from company Y to be delivered by rail. Y prepares an electronic manifest-of-record from the bill of lading for 100 RFID tagged pallets of widgets. For simplicity, we'll use UHF active RFID tags because we're going to scan the pallets (or rail cars, or boxes, or individual widgets for that matter) in motion and at distance. Needless to say, there is a GPS transponder on each rail car to transmit current coordinates to a central tracking system. All of this data is integrated in real time with continuous comparison with our electronic manifest-of-record.

Can you spot the weaknesses of this system? Note that verification breaks down if any one of the following takes place: (a) the GPS transponder is compromised, (b) the GPS transponder is moved, (c) the RFID tags are electronically destroyed (e.g., via an electronic pulse bomb or microwave beam), or, and this is the money shot, (d) the RFID data is corrupted!

The real payoff for the sophisticated criminal or terrorist is a combination of (c) and (d) because it's so easy. Here's how it might work. RFID tags are easy to destroy electronically. Suppose that the original RFID "widget" tags are electronically neutralized and replaced with tags that report their contents to be "anti-widget" - not a terribly difficult thing to do. Now, our system reports that rail car loads of "anti-widgets" are moving toward company X. Let's take this one step further. Suppose we put our own RFID "widget" tags on pallets of explosives and load that on the rail car somewhere along the line. Now our system reports rail car loads of widgets are moving toward company X, when in reality rail car loads of explosives are moving toward company X. You get the point. The vulnerability is that there is no way to validate that the RFID report of the contents to which it is attached is accurate. If you think about it, this is the same problem our friend the civil engineer had in conceptualizing what prox cards do. Unless RFID data is biometrically, chemically, or physically "connected" with the tagged contents, the system is not foolproof. In fact, it's nearly trivial to spoof. Don't believe it. Watch a demo of how easy it is to compromise an RFID security system on YouTube.

You might say, but my RFID systems MiFare security built-in. Sorry, chum, but Mifare got hacked in 2007. The system compromised in the YouTube video had MiFare enabled! Bottom line: RFID is a very useful technology, but it's vulnerable to hacking and spoofing just like WiFi. You might not want to bet the bank on it. You could get caught with your chips down. Oh, and for those of you who think electronically opaque wrappers solve the problem, note that this also undermines tracking!

Hal Berghel is Associate Dean of the Howard R. Hughes College of Engineering at UNLV and Director of the new UNLV School of Informatics. He is also Director of the Identity Theft and Financial Fraud Research and Operations Center. His consultancy, Berghel.Net, provides security and management services to government and industry.