



RFIDIocy: It's Déjà Vu All over Again

Hal Berghel

University of Nevada, Las Vegas

Not content with pedestrian applications, some manufacturers extended RFID far beyond the level justified by good taste and common sense.

One of the social glues that bonds baby boomers together is AM radio. Not the current AM talk show radio babble, but the good stuff of yesteryear: Chicago bluesmen, rockabilly, and iconic American rock-and-roll bands like the Zombies, Traffic, and the Spencer Davis Group.

Howard Duff as Sam Spade, the Lux Radio Theater, and the Cisco Kid brought us together with shared experiences that were staples of daily life in that bygone era. *Yours Truly, Johnny Dollar*; *Boston Blackie*; Sonny Boy Williamson II on the *King Biscuit Time*; and the Grand Ole Opry on Nashville's WSM 650 did it for me. We could get a taste of life in the distant lands and exotic places on the other end of the signal.

For a variety of reasons, this format only lasted a few years—from radio's inception in the early 20th century through the 1950s, when modern transportation removed much of the curiosity inherent in the experience, and a displacing technology called TV caught on.

But those of us who remember old time radio are indebted to one inconvertible law of physics: radio frequency signals don't obey property lines. Hold that thought for a moment.

NOT EVERYTHING WE CAN DO IS WORTH DOING

There has never been a shortage of bad ideas. But there are bad ideas, worse ideas, and what I'll call the "estupidísima." Some purposes for which we've used radio frequency identification (RFID) fall into the latter category.

A posteriori bad ideas are those that seemed reasonable enough at the time but failed at the level of implementation. Examples might include New Coke, the Microsoft Bob operating system, the IBM PCjr, and the Edsel. They just didn't catch on—not because of some fundamental flaw, but rather because they targeted a nonexistent need or misjudged a market. A posteriori bad ideas produce responses like, "I'm not actually seeing this" or "This isn't ready for prime time."

"Estupidísima" ideas are a special class of a priori bad ideas. They enjoy a status in the world of suboptimal decision making. Examples include placement of the Ford Pinto fuel tank close to the rear bumper, the installation of untested blowout preventers in deep water oil exploration, and building bridges in high-wind areas while failing to embrace the notion of aeroelastic flutter. Conceptually flawed a priori bad ideas usually produce questions like, "What were they thinking?" or, perhaps, "What were they smoking?" These are the superfund sites of stupid. They may be identified by one or more of the following red flags:

- Industry associations and oversight groups either fail to warm up to them, or are critical of them, early on in their gestation.
- The wisest of investors tend to shy away from them.
- Rollouts are frequently unpredictable and rocky.
- Criticism, embarrassment, litigation, or hacks evolve in parallel with the implementation.

CURRENT APPLICATIONS OF RFID TECHNOLOGY

R RFID technology is used for automatic identification and tracking in a wide variety of applications, including the following:

Automotive industry

- Vehicle immobilizers
- Inventory management
- Agile and flexible manufacturing
- Product life-cycle management

Cattle ranching and animal tracking

- ID tags
- Timing pigeon races

Healthcare

- Patient tracking
- Tracking of high-value pharmaceuticals
- Resources management
- Internal appliance ID
- Human implants using VeriChip

Manufacturing

- Supply-chain management
- Warehousing
- Asset management
- Inventory control

Defense

- Logistics and inventory control
- Field combat

- Marking of high-value assets as well as targets
- Identification, friend or foe (IFF) aircraft detection
- Reconnaissance

Retailing

- Inventory and shelf management
- Tracking point-of-sale information
- Information kiosk and customer service
- Loss prevention
- Customer loyalty programs

Transportation

- Electronic toll collection
- Automatic vehicle identification
- Fleet management
- Car parking and access control
- Electronic vehicle registration

Marine terminal operation

- Container tracking and handling

Other applications

- Payment transactions
- Casino chip tracking
- Library management
- IDs such as enhanced driver's licenses and passports

Source: www.berghel.net/publication/rfid/rfid.pdf

- Eventually, they become part of the literature on ecological nightmares, engineering disasters, and the like, and, if dumb enough, will eventually be featured in eponymous documentaries.
- They tend to be career stoppers for the principals involved.

A recent example of an exceedingly bad idea is the use of RFID in security-challenging applications. The operative part of RFID is RF—the very phenomenon, you might recall, that doesn't obey property lines.

RFID

RFID technology uses radio frequency transmissions to exchange information between a “tag” (aka,

transponder) and an interrogator (aka, reader) via middleware that supports the interface between the RFID hardware and the applications software.

The RFID concept isn't new. Leon Theremin of electronic musical instrument fame invented one progenitor in the 1940s. This device, called “the Thing,” was a passive cavity resonator that derived its power from an RF signal provided by an external transmitter.

Requiring no internal power source, the Thing was easy to conceal and difficult to detect, thus it became useful in spying. In fact, the Russians used this technique to bug the Moscow office of US Ambassador W. Averell Harriman. The Thing was embedded in a wooden plaque of the Great Seal of the United States

presented to Harriman by a Soviet “good will” organization. The plaque continued to broadcast conversations from the ambassador's office until 1952, when it was discovered accidentally by a British amateur radio operator who overheard some office conversations.

There's a second lesson here, folks: RF not only doesn't obey property lines, it also doesn't respond well to authority.

Flash forward 50 years: the Thing has evolved into an inexpensive and more capable alternative to bar code recognition for asset management, inventory control, point-of-sale systems, pet identification, high-value chip control in the gaming industry, firearms, and the list goes on and on. As the “Current Applications of RFID Technology” sidebar indicates, if there's a need to know what something is, or where it is, RFID technology is ready and waiting.

Not content with pedestrian applications, some manufacturers extended RFID far beyond the level justified by good taste and common sense. RFID has now found its way into the holy trinity of security: authentication, validation and verification. They just couldn't leave good enough alone. Over the past decade or so, RFID tags have become nearly as ubiquitous as name tags.

RFIDIocy

Simply put, RFID isn't a great choice for single-token verification/authentication mechanisms—they're both too noisy and too easy to hack. The reasons are obvious and subtle. I'll illustrate with two examples, both applications being spectacular in their foolishness.

Keyless entry and transit passes

Most of us are familiar with using transit pass and keyless entry applications while commuting or for office building access. This

application was wrapped around the concept of convenience, pure and simple—for users, managers who feel more comfortable with a steady stream of exception reports, and the people who maintain access logs. But it wasn't wrapped around the security concept.

Imagine the appeal of boarding a bus or accessing a building without so much as a card swipe. One such solution is the NXP Mifare DESFire RFID smart card. Mifare is the encryption standard used, and NXP is the Philips Electronics subsidiary that makes the card. This technology was exceedingly popular for nearly a decade—at least until 2011, when virtually everyone with any interest knew how to hack it. However, this isn't an a posteriori bad idea—it's a serious contender for *estupidísima* status. Why? Because the system was built around a known vulnerability that was understood as far back as 1999.

There's no shortage of online resources for information about cracking Mifare RFID cards in a variety of settings, from transportation tokens to key vaults. In his blog at www.schneier.com/blog/archives/2008/08/hacking_mifare.html, security expert Bruce Schneier referred to Mifare Classic security as “kindergarten cryptography” (www.schneier.com/blog/archives/2008/08/hacking_mifare.html).

The nail in NXP DESFire's coffin came from a “template attack,” a specific type of side channel attack, which showed that further resistance to hack attacks was futile. The “Side Channel Attacks” sidebar provides more information about these techniques for breaking cryptographic systems. A discussion of template attacks, including links to source documents, can be found at <http://arstechnica.com/business/2011/10/researchers-hack-crypto-on-rfid-smart-cards-used-for-keyless-entry-and-transit-pass>.

SIDE CHANNEL ATTACKS

Working with his colleagues at Cryptography Research in the late 1990s, Paul Kocher, one of the SSL 3.0 architects, developed techniques for breaking cryptographic systems, called side channel attacks (www.cryptography.com). The basic idea was to use the system's physical characteristics against itself. Kocher observed that by monitoring power consumption, timing frequencies, electromagnetic propagation, acoustic signals, and so on, it's possible to gain enough information about processor operation to recover keys and messages.

The earliest side channel attacks like simple power analysis required some under-

standing of the circuits involved. More powerful side channel attacks such as differential power analysis and high-order differential power analysis use advanced statistics and are largely circuit insensitive.

Kocher's research went viral, and subsequent researchers have proven the viability of his concept in scores of professional publications. The technique of using “compromising emanations” to gain intelligence from electronics was the stuff of which the National Security Agency's Tempest project in the 1970s was made (www.wired.com/threatlevel/2008/04/nsa-releases-se).

PASS cards

As ill-conceived as DESFire was, it pales in comparison to the people access security service (PASS) card. L-1 Identity Solutions, which French defense contractor Safran acquired in 2011, manufactures PASS cards, which are designed to provide a single document verifying both identity and citizenship as now required by US law. This was a mistake carried through to digital perfection if ever there was one.

The concept is simple enough. Millions of people cross US borders each year. Wouldn't it be nice if we could speed up the process and detect potential threats as far away from the turnstile as possible? I'm sure you see where this is headed. That's right, the Department of Homeland Security (DHS) selected RFID as the solution of choice. Immediately following the announcement, trade groups such as the Smart Card Alliance pointed out that RFID was not the best fit because its use raised security and privacy concerns.

The original State Department RFID for the PASS card system was released in 2006 (www.homelandsecuritynewswire.com/state-department-issues-rfi-whiti-pass-card-system.) A Smart Card Alliance press release critical of

the use of RFID in PASS cards followed quickly thereafter (www.smartcardalliance.org/articles/2006/06/08/smart-card-alliance-challenges-dhs-stand-on-deploying-rfid-for-whiti-pass-card)—three years before the cards were put into service. A short DHS description and video showing the PASS card's intended use are available at www.getyouhome.gov/html/rfid/rfid_how_to.html. A comparison of this video with the one at www.youtube.com/watch?v=NW3RGbQTLhE should prove illuminating.

The problem is twofold. From a privacy perspective, even if it's encrypted, it's not the best idea to broadcast data that is used in identification. From a security perspective, this is an invitation for RFID spoofing—hacking the system to produce bogus credentials so the bad guys look like good guys. What every narcotics trafficker and terrorist needs is a bogus RFID tag that takes on a persona with saint-like qualities.

RFID spoofing is as old as RFID itself. Spoofing wasn't perceived as a problem in the earliest RFID applications because so little was at stake. After all, what was the likelihood that someone would spoof RFID tags to mess up a grocer's inventory control system?

However, the PASS card presented an opportunity to put RFID spoofing to important use.


Of course, the proponents of this ridiculous use of RFID pointed to DESFire EV1, the uber-secure, 20-year-old RFID security standard embedded in the Mifare Classic cards. But before the first batch of PASS cards was even manufactured in spring 2008, at least one hack was presented at the Chaos Communication Congress in December 2007 (www.linux-magazine.com/Issues/2007/77/Chaos-Communication-Congress). In addition, an actual attack was demonstrated on YouTube (www.youtube.com/watch?v=NW3RGbQTLhE) in February 2008—several months before the PASS card became an official standard. It's useful to compare this YouTube video with the NXP pro-

motional video produced just a few months earlier (www.youtube.com/watch?v=teKBR0BvuLU).

The PASS card remains in use, but it's my understanding that DHS is no longer confident in it as a source of trusted identity. By the way, the DHS solution to the RFID spoofing problem was to place the RFID card in a metallic sleeve. Of course, this eliminates the advantage of RFID over more secure options like smart cards—which is pretty much what the Smart Card Alliance pointed out to Congress before the rollout.

The unsuitability of RFID for secure applications has been understood as long as the technology has been available. Although it's obvious that using RFID in secure applications isn't appropriate, the RFID industry continues to squelch disclosures

of vulnerabilities by trying to suppress technical publications and presentations, and even TV shows—for example, Adam Savage of *MythBusters* fame refers to such RFID censorship at www.youtube.com/watch?v=-St_ItH90Oc.

For an overview of RFID and concomitant security issues, see www.berghel.net/publications/rfid/rfid.pdf. 

Hal Berghel, Out of Band column editor, is a professor of computer science at the University of Nevada, Las Vegas, where he is the director of the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). Contact him at hlb@computer.org.

 Selected CS articles and columns are available for free at <http://ComputingNow.computer.org>.