

Sponsored By

SPECTRUM

RFID inside

By: **Kenneth R. Foster** and **Jan Jaeger**

PHOTO: GUSTO IMAGES

Wanted: Power-systems engineer with experience in high-power (5–100-kW) motor-controller design. Must be U.S. citizen and have valid ISO1443-compatible access-control RFID implant.

Sound farfetched? Today, yes. A decade from now, maybe not.

With the proliferation of radio-frequency identification technology and the recent, but increasing, use of implantable RFID chips in humans, we may already be on a path that would make such an ad commonplace in a 2017 issue of *IEEE Spectrum*.

The benefits would be undeniable—an implantable RFID chip, which is durable and about the size of a grain of rice, can hold or link to information about the identity, physiological characteristics, health, nationality, and security clearances of the person it's embedded in. The proximity of your hand could start your car or unlock your front door or let an emergency room physician know you are a diabetic even if you are unconscious. Once implanted, the chip and the information it contains are always with you—you'd never lose your keys again.

But there is a darker side, namely the erosion of our privacy and our right to bodily integrity. After all, do you really want to be required to have a foreign object implanted in your arm just to get or keep a job? And once you have it, do you really want your employer to know whenever you leave the office? And do you want every RFID reader—equipped supermarket checkout counter to note your presence and your purchases?

Until a couple of years ago, chipping humans was largely the domain of cybernetics provocateurs like Kevin Warwick or hobbyists like Amal Graafstra [see Graafstra's accompanying article, "[Hands On](#)"]. Then, in 2004, the U.S. Food and Drug Administration, which regulates medical devices in the United States, approved an RFID tag for implantation in humans as a means of accessing a person's health records.

This tag, called VeriChip, is a short-range transponder that relies on the signal from a reader unit for its power supply [see photo, "Anatomy of an RFID Tag"]. When exposed to a varying magnetic field from the reader, the chip powers itself up and repeatedly transmits a 16-digit code that is unique to the tag. According to the company, 2000 people have already had tags implanted.

The VeriChip tag is part of a health information system called VeriMed. The code contained in the implanted chip points to a record in a database identifying the patient and containing that patient's health records. By scanning a person's chip, caregivers can retrieve an identification code that enables them to access the medical history of people who cannot otherwise communicate their identities—speeding up their treatment and possibly saving their lives.

VeriChip Corp., a subsidiary of Applied Digital Solutions, headquartered in Delray, Fla., is also promoting its device as a security measure. It has six clients around the world, five of which use the implant as a secondary source of authentication, says Keith Bolton, vice president of government and international affairs for VeriChip. The highest-profile example of this application came in 2004 when the attorney general of Mexico and 18 of his staff had chips implanted to allow them to gain access to certain high-security areas.

The tag is also finding use as a kind of implanted credit card. In trendy nightclubs in the Netherlands, Scotland, Spain, and the United States, patrons can get “chipped”—at a cost of about US \$165 in one establishment. In future visits, “by the time you walk through the door to the bar,” one proprietor told Britain’s Daily Telegraph, “your favorite drink is waiting for you, and the bar staff can greet you by name.”

And the list of proposed applications could grow quickly. VeriChip is advancing a scheme to “chip” soldiers, as a replacement for a soldier’s traditional dog tag, and a VeriChip officer has proposed chipping guest workers entering the United States.

Before too many of those suggestions become realities, we need to examine carefully the very real dangers that RFID implants could pose to our privacy and our freedom. If we don’t figure out the risks and come up with ways to mitigate them, someone answering that ad for a power engineer may live in a world with considerably less privacy and feel compelled to have an implant just to be able to get a job.

The VeriChip tag’s main use, as a means of identifying patients who might be unable to communicate with caregivers and of accessing their medical records, could clearly be lifesaving in emergency situations. As long as the patient has provided informed consent and the privacy of the patient’s medical records is adequately protected, there are few ethical concerns with the technology. But VeriChip Corp.’s well-meaning attempt to improve personal health care may serve as a beachhead for wider use, and that expansion could create urgent ethical issues, particularly if an element of coercion enters into the process.

Consider, for example, a proposal by Scott Silverman, CEO of VeriChip. In an interview on 16 May 2006 on Fox News Channel (a U.S. television network), he proposed implanting chips in immigrants and guest workers to assist the government in later identifying them. Shortly afterward, the Associated Press quoted President Álvaro Uribe of Colombia as telling a U.S. senator that he would agree to require Colombian citizens to be implanted with RFID chips before they could gain entry into the United States for seasonal work.

Guest workers might ostensibly consent to having chips implanted. But would chipping them be truly voluntary? Such “voluntary” actions may determine a person’s ability to earn a living, and the worker might not view the implantation as something he or she could refuse. What person facing poverty at home and given the prospect of a job in a different country would be in a position to argue?

At a practical level, when chips are implanted in guest laborers, who pays for the cost of purchasing, implanting, and monitoring the chips in hundreds or thousands of poor migrants? If someone has an adverse reaction to the chip so that it has to be removed or replaced, who bears that cost? And who pays if the chips become obsolete or compromised by rampant cloning—the illicit duplication of the supposedly unique device—and have to be replaced? Affluent patrons of a trendy club might gladly pay to be chipped, but the situation would certainly be different for those pursuing temporary minimum-wage jobs in a foreign country.

Silverman made his proposal, that immigrants and guest workers be implanted with RFID chips, amid a national debate in the United States about illegal immigration, focusing on impoverished Latin Americans in search of work. But might Silverman’s proposition apply as well to electrical engineers or doctors, or other high-status individuals coming into the country for work? Who decides?

Mandating guest workers to have RFID chips implanted in their bodies for identification purposes strikes us as coercive and opportunistic. That approach makes the RFID chip a branding device similar to what a cowboy uses when he sears the haunches of his cattle or the tattoos that the Nazis forced on their victims in concentration camps. It goes against the widely held belief in basic human rights and might even be interpreted as a violation of Article 3 of the United Nations’ Universal Declaration of Human Rights, which affirms everybody’s right to “life, liberty, and security of person.”

Social researchers are just beginning to study people’s attitudes to implanted RFID. Christine Perakslis and Robert Wolk at Bridgewater State University, in Massachusetts, questioned 141 college students on their feelings about implanted RFID. Respondents were asked if they would be willing to have an implant to prevent ID theft, to combat terrorism, for other national security reasons, as a life-saving device, or to ensure the safety of themselves and their families. About a third of the respondents were willing to be implanted, while less than half of them were not. Wolk and Perakslis’s subjects were the least comfortable with chipping as a cure for ID theft. The reasons that garnered the most support for getting chipped were to save their lives or to ensure the safety of their family.

“If they are putting something inside of you,” one respondent replied, “it’s like you’re changing yourself. It’s not right”

Another small survey in 2003 by Starr Roxanne Hiltz, professor of information systems at the New Jersey Institute of Technology, in Newark, and her colleagues found that 18 out of 23 people questioned objected to the idea of implantable chips as identification.

Some of the resistance has to do with feelings about modification to one's body. "If they are putting something inside of you," one respondent replied, "it's like you're changing yourself. It's not right." As the wide variety of acceptable and unacceptable piercings and tattoos found around the world attests, people of different backgrounds vary in their attitudes toward "changing yourself."

Tattoos, an ID technology that is at least 4000 years old, share some key qualities with implanted RFID tags. Both could be used for the same purposes and are intended to be permanent—they can be removed, but only with some difficulty and not without assistance. The only differences are that, compared with a tattoo, an RFID chip is invisible, may be easier to read surreptitiously, and is a little more difficult to duplicate. Yet we suspect most people, regardless of their feelings toward being chipped, would balk at the idea of accepting a machine-readable tattoo as a means of identification, even if such an indelible marking had some personal or societal benefit.

If there were a societal benefit, could a government require individuals to modify their bodies? For public health purposes, the answer is yes. In the United States, for example, students must have certain immunizations before attending public school. But this example is the only instance we can think of. Could a health care-related implant such as the VeriChip tag become a public health imperative? Would that use lead down a slippery slope toward universal chipping? It seems unlikely.

VeriChip Corp. does not, in fact, advocate universal chipping for medical purposes. The company's vice president of medical applications, Richard Seelig, estimates a U.S. market for VeriMed of 43 million to 45 million people—less than one-sixth of the population. This group is made up of people who are more likely than others to wind up in the emergency room. These include cancer patients undergoing chemotherapy; people with pacemakers or other medical implants; and those who might be suffering some sort of cognitive impairment or loss of consciousness due to epilepsy, diabetes, or Alzheimer's disease.



PHOTO: ORAN BARBER/BETH ISRAEL DEACONESS MEDICAL CENTER

TEST CASE: Dr. John Halamka [right] got chipped. He later helped expose a weakness in VeriChip's security.

We believe that even Seelig's estimates of the potential size of the market for patient identification are grossly exaggerated. "For certain subpopulations—Alzheimer's patients, the mentally ill, people with communication difficulties—having an implanted identifier makes great sense," says John Halamka, a former emergency physician and now CIO at Beth Israel Deaconess Medical Center, in Boston. "Others can just carry a card in their wallet, a medic-alert bracelet, or a USB drive with their personal health records. There is no clear medical or business justification for chipping large populations of healthy people."

In fact, so far there is no clear evidence that the VeriChip will help patients facing medical emergencies. The first study designed to determine whether patients, physicians, and insurers benefit at all from VeriChip began only last fall, in New Jersey.

Other nonimplanted technologies based on RFIDs may soon provide some of the benefits to the patient VeriChip hopes for. For instance, nonprofit health care informatics organization MedicAlert is researching RFID-enabled bracelets that would link to a personal health care record. However, as with VeriChip, a key question is how to ensure the privacy of the information in the databases, while at the same time providing easy access to the database by caregivers in emergency situations.

A right to privacy is at the heart of some of the questions raised by implanted RFID tags. In agreeing to be chipped for medical purposes, the patient gives up a measure of privacy for his or her own potential benefit. But when chipping is used for other reasons, difficult confidentiality issues can arise. When a business gives an identity card to a newly hired worker, for example, the company retains ownership of the card. But will the employer also own the chip inside an employee's body?

A test case may be on the horizon: the first U.S. company to implant employees with VeriChip, CityWatcher.com, in Cincinnati, recently closed its doors. Its CEO, Sean Darks, himself an implantee, did not return repeated phone calls inquiring whether employees kept their implants after the company folded. VeriChip itself makes no recommendation about whether former

employees should be “dechipped,” says the company’s Bolton. But he says removal is a quick and easy procedure. “I’ve had many [chips] in and out of my body,” he says.

Perhaps just as important a question as who owns the chip is that of who owns the data on the chip. Can the tag be read and its data used without the consent of the person who has it implanted?

Fears that some individuals have expressed about being tracked through an implanted chip are probably unrealistic. The VeriChip and most other passive RFID devices, those that derive their power from the reader, provide only an identification number and can be probed only from very short distances. The VeriChip is readable only at 10 centimeters or less using its handheld scanner.

This distance can be increased, however, using more efficient antennas. Digital Angel Corp., in St. Paul, Minn., also owned by VeriChip’s parent company, Applied Digital Solutions, is developing a “walk-through” scanner with greater range. Nevertheless, the prospects of a “drive-by” theft of a person’s identity seem remote, and even more remote is the possibility that the government or some other organization might track an individual moving about in ordinary life.

Still, if the computer age has one lesson, it is that systems and data are invariably less secure than their proponents claim. Particularly troubling for a device that is being marketed for access control, the VeriChip lacks modern cryptographic and other protections and is prey to simple attacks [see online sidebar, “How VeriChip Works...and Doesn’t ”]. In a recently published article in the Journal of the American Medical Informatics Association, Beth Israel’s Halamka and colleagues showed how easily a simple-to-build device can scan the chip and replay the radio signal to fool a VeriChip reader [see “Test Drive”].

This flaw may be insignificant when the chip is being used for identification purposes—for example, with an Alzheimer’s patient. But Halamka and his coauthors argue forcefully that the chip should not be used for authentication purposes to control access to sensitive areas or information.

Though for now they store nothing more than a number, inevitably, implanted RFID chips will store more data and databases will be created that link information on implanted chips to other facts about a person. It is easy to foresee situations in which even a simple identification number might lead to harm—consider the millions of dollars lost to identity theft in the United States because of the disclosure of Social Security numbers and similar data.

So what can we do about implanted RFID’s impending problems? Using legislation to restrict their use is an obvious measure; in fact, laws are already in the works. Faced with widespread public concerns about this technology, more than 10 U.S. states have enacted laws limiting implants. In May 2006, for example, Wisconsin passed a bill that would prohibit requiring anybody to have a microchip implanted.

But laws might be difficult to enforce if implanted chips, like drivers’ licenses, remain voluntary but become de facto requirements for many kinds of employment or services. And the Wisconsin law does nothing to allay worries about the loss of privacy. Governments may need to make the unauthorized reading of an implanted RFID tag illegal as well.

Some of the ethical concerns can be addressed with better technology. Ari Juels, head of RSA Laboratories, the R&D arm of RSA Security, in Bedford, Mass., believes that, with proper encryption methods, a person’s privacy can be preserved without decreasing the usefulness of the implant. Juels says that the ease with which a thief can steal a VeriChip radio signal makes the tag a poor security tool, but that it eliminates a thief’s incentive to kidnap or carve someone up. So together with Halamka and others, he developed a technique that still lets a thief copy the chip’s radio signal but at the same time keeps the actual ID number it represents safe. Lest you think criminals would not go to such extremes, in 2005 BBC News reported that thieves stole a car protected by a fingerprint-reading lock by chopping off the owner’s finger.

Halamka’s solution, by the way, would make it impossible to track an implanted individual by noting which RFID readers—at stores, doors, gas pumps—picked up his or her radio signature. Crucial to Juels’s technology is that the chip’s radio signature changes unpredictably each time it’s read, even though the bits it encodes remain the same.

But maybe the ultimate solution, to allow accurate identification of individuals without some of the ethical issues raised by implanted radio chips, might require a different technology completely—biometric scanners. Although such devices are more costly than RFID-chip readers, they will inevitably become more affordable with time. And the “tags” are always going to be more competitive: after all, we have all already been issued our fingerprints.

About the Author

KENNETH R. FOSTER, an IEEE Fellow, is a professor of bioengineering at the University of Pennsylvania, in Philadelphia, and a former president of the IEEE Society on Social Implications of Technology. JAN JAEGER is a former emergency room nurse who teaches at Penn’s School of Nursing and was a fellow at the university’s Center for Bioethics.

To Probe Further

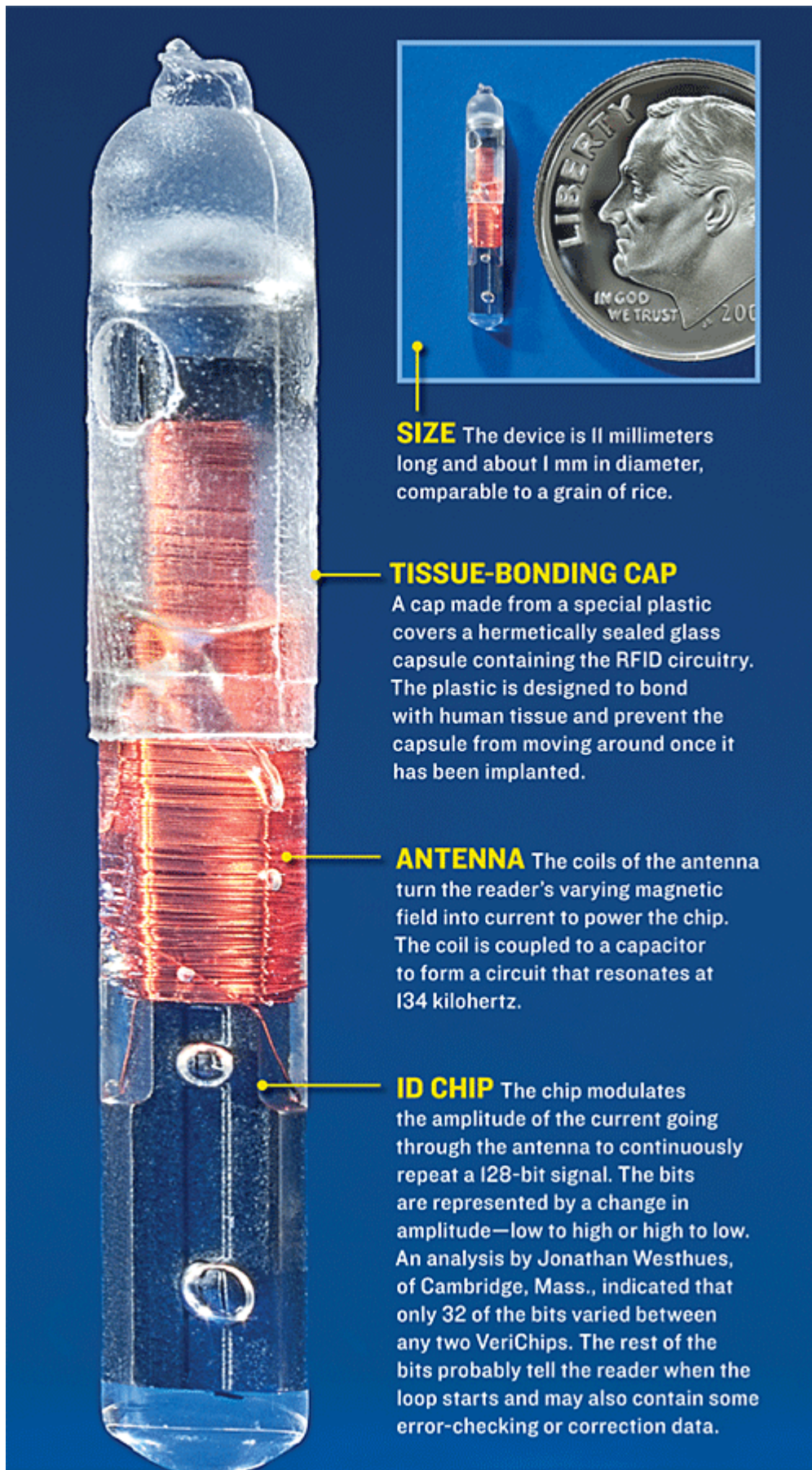
To get a grasp of how people feel about implanted RFIDs, see “Social Acceptance of RFID as a Biometric Security Method,” by Christine Perakslis and Robert Wolk, IEEE Technology and Society

Magazine, Fall 2006.

Katina Michael, a lecturer at the University of Wollongong, in Australia, has examined the societal implications of RFID implants and related technologies. See <http://ro.uow.edu.au/kmichael>.

A major technical conference, IEEE RFID 2007, will be held in Grapevine, Texas, from 26 to 28 March.

Figure 1



SIZE The device is 11 millimeters long and about 1 mm in diameter, comparable to a grain of rice.

TISSUE-BONDING CAP

A cap made from a special plastic covers a hermetically sealed glass capsule containing the RFID circuitry. The plastic is designed to bond with human tissue and prevent the capsule from moving around once it has been implanted.

ANTENNA The coils of the antenna turn the reader's varying magnetic field into current to power the chip. The coil is coupled to a capacitor to form a circuit that resonates at 134 kilohertz.

ID CHIP The chip modulates the amplitude of the current going through the antenna to continuously repeat a 128-bit signal. The bits are represented by a change in amplitude—low to high or high to low. An analysis by Jonathan Westhues, of Cambridge, Mass., indicated that only 32 of the bits varied between any two VeriChips. The rest of the bits probably tell the reader when the loop starts and may also contain some error-checking or correction data.

ANATOMY OF AN RFID TAG: The VeriChip implantable RFID tag, shown below, is the only tag approved for use in humans for a medical application. It is a simple device consisting of a coil of wire and a hermetically sealed microchip within a glass capsule. The coil acts as an antenna and uses an RFID reader's varying magnetic field to power the microchip and transmit a radio signal. Each VeriChip's signal is a unique identifying number that links to a medical record database.

PHOTO: LESTER LEFKOWITZ (2)

Sidebar 1

How Verichip Works...and Doesn't

A shopper collapses at a grocery store. Alive but unresponsive, he is rushed to the emergency room of a local hospital. Seeing that the patient is emaciated and nearly hairless, doctors suspect that the man is undergoing an aggressive form of chemotherapy. But what drug is being used? Who is his personal physician? What other complications might be expected?

VeriChip, the first human implantable RFID chip approved for medical use in the United States, was intended for just such a situation. If the unfortunate fellow had been implanted with a VeriChip tag, and if he had the luck to be wheeled into a hospital that follows VeriChip's suggested protocols, emergency room staff would scan his upper arm with a reader device while taking his vital signs.

The reader would then detect the unique 16-digit number the chip transmits and plug this identifier into a database, called VeriMed. Through VeriMed, the staff could obtain personal health information that the patient himself has provided, such as what drugs he is on and why, contact information for his physician, and possibly a link to the records at the hospital at which he is usually treated. Physicians in the emergency room would not have to waste time running unneeded diagnostic tests and could treat him faster and without fear of causing a deadly drug interaction.

The chip consists primarily of a coil of wire that acts as an antenna and a microchip capable of generating a radio signal that encodes 128 bits of information and is readable from, at most, centimeters away. The reading device emits a magnetic field that oscillates at a frequency of 134 kilohertz. The reader and the chip's antenna basically form a transformer, turning the oscillating magnetic field into current in the implant.

Most of what's known outside of VeriChip Corp. and its supplier, Raytheon's Spanish subsidiary, comes from the RFID hobbyist Jonathan Westhues. In 2005, journalist Annalee Newitz approached Westhues and asked him to try to spoof—to create a tag that gives off an identical radio signal—the VeriChip that she'd had implanted for a story in *Wired*.

For a device that is marketed as part of an access-control and security application, VeriChip was distressingly easy to mimic. Westhues had already built a digital RFID reader, which he called the Proxmarkii, when Newitz contacted him. Using his reader, he was easily able to turn Newitz's chip on, record and analyze the signal emitted, and then reproduce that signal—tricking an actual VeriChip reader into believing it was querying Newitz's implant.

Westhues performed some further work with security expert Adam Stubblefield, an assistant research professor at Johns Hopkins University; with Ari Juels, head of security skunkworks at RSA Laboratories, in Bedford, Mass.; and with John Halamka, CIO of Beth Israel Deaconess Hospital, in Boston, and a VeriChip implantee.

Here's what they found: when subjected to a 134-kHz magnetic field, the VeriChip will repeat a 128-bit message continuously for as long as the probe signal lasts. Although Westhues had only a handful of VeriChips to work with, among those few, only 32 of the bits varied. Those 32 existed in two chunks of 16 bits each. Westhues and his colleagues suppose that the remainder of the bits include a sequence that tells the reader when the 128-bit loop starts as well as some sort of error-checking or -correcting data.

The bits are encoded using what's called Manchester-coded amplitude-shift keying. Amplitude-shift keying means simply that the bit is represented by a change in the amplitude of the radio wave. Manchester coding means that the direction of the amplitude change—low to high or high to low—is what counts, rather than the actual amplitude.

From a security standpoint, VeriChip's only advantage over the RFID key that's probably in your pocket right now is that you can't lose it. Unlike some other RFID key signals, the radio signal the VeriChip emits does not change each time the tag is energized; so once you've read the chip, you can simply play back the signal you picked up and pretend to be in possession of the chip.

Westhues offered this analogy. Most security is achieved by putting a padlock on something. What security VeriChip offers is more akin to bolting something down with a five-sided bolt instead of a normal six-sided bolt. A standard wrench won't be able to unbolt it, just as a standard reader won't be able to understand a VeriChip. But a less specialized tool could easily unscrew the bolt, just as Westhues's general RFID reader allowed him to detect and play back the chip's signal.

Westhues is thus unimpressed with the chip. "I'd say that in great part, everything about VeriChip has been sensationalism over reasonableness," says Westhues. "Once, instead of carrying a tag in your wallet, you implant it, things get funny. People stop thinking about the technical limits. People imagine that they're more complex than they are."

Though he confirms that the technical details are correct, Richard Seelig, VeriChip's vice president for medical applications, is, naturally, critical of the group's conclusions about the

chip's vulnerability. He argues that although these outsiders were able to spoof chips in the lab, they did not attempt to steal a VeriChip radio signal in the field, and so did not prove that such an attack is possible. He adds that when used as part of a security and access-control system, the signal from a VeriChip would not be the only authentication. A key code or some other kind of PIN would also be required.

VeriChip vice president for government and international affairs Keith Bolton, who handles the company's security business, says there is a plan to add more security to VeriChip, but would not elaborate.

RSA's Juels counters that the tests he and his colleagues carried out "were sufficient to demonstrate a fundamental vulnerability to cloning attacks." Even if they'd tried such attacks in the field, the only information they might gain would have to do with how far away you could be from the scanner and still clone a VeriChip signal. Also, Juels says that none of his implant-spoofing pals are antenna designers, so the information might not be the best anyway.

Juels is equally dismissive of Seelig's argument that the VeriChip would never act as a key on its own. "That the VeriChip may be secure when buttressed with another authenticator is, in my view, cold comfort," says Juels. "Parachute manufacturers do not justify defects in their products by arguing that skydivers generally carry two parachutes." That said, he acknowledges that many common secondary authentication devices, such as four-digit PINs used in many automated bank teller machines, are known to be insufficient on their own. But, he adds, at least their users recognize the limits and try to compensate for them.

Only time will tell whether VeriChip Corp. has a future in the access-control market, but the company is certainly working to advance its medical business. This past October, Digital Angel Corp., a separate firm within the holding company that owns VeriChip Corp., was granted a U.S. patent on an implantable RFID chip that reads and transmits blood glucose levels. That would free many diabetics from having to lance their fingertips to keep track of their blood glucose levels and insulin needs. The company says such a device could enter clinical trials as early as November. "It would take VeriMed to a completely different level," says Seelig. "...what the biosensing would do is let us not just tell who you are and some things about you, but tell how you are as well."

—K.R.F. & J.J.