

Sponsored By

**SPECTRUM**

## Hands On

By: **Amal Graafstra**

PHOTO: AMAL GRAAFSTRA

An X-ray shows Amal Graafstra's hands with implanted RFID tags.

When I open my front door, I don't reach for a key. When I log into my computer, I don't touch my keyboard. When I start my motorcycle, again, no key needed. Instead, I just wave my hand and I'm in business.

I was one of the first do-it-yourselfers to have a radio-frequency identification (RFID) tag implanted under my skin. In fact, I have two—one between the thumb and index finger in my left hand, the other in the matching spot on my right hand.

So what's a nice guy like me doing with a microchip in each of my hands? My life as an RFID guinea pig started in early 2005. At the time I was managing servers for medical facilities around Seattle, a job for which I carried around a ring of keys to almost 100 different doors and drawers.

That bulky key ring got me thinking. It struck me that modern keys are just crude identification devices, little changed in centuries. Even if each lock were unique—most aren't—keys can be copied in any hardware store and, once distributed, are hard to control.

I considered biometric authorization, in which access is granted only if a scanned physiological trait, such as a fingerprint or the pattern of an iris, matches a pattern stored in a database. But I found biometrics to be neither cheap nor reliable, so I turned my attention to RFID—specifically, the access card systems commonly found in office buildings.

Two weeks later, I was sitting in a doctor's office. After sterilizing the tiny glass cylinder, the doctor injected a small amount of local anesthetic to numb my left hand. She made a 2-millimeter incision in the fleshy part next to my thumb, lifted the skin, and slipped the tag inside. She applied some skin glue and bandaged it up. Just like that, I became one of the few people on Earth walking around with a radio transponder in my hand.

**In an RFID "lock" system**, each RFID tag, which is essentially a minitransmitter, sends out a sequence of radio-frequency pulses representing a unique number, usually 10 to 16 digits in length. An RFID tag's memory typically ranges from a few bits to 128 bits, in the common ISO-compliant tag, to several megabytes. The locks are programmed with a list of authorized numbers; if your tag emits one of those numbers, you're in. If not, you're not. If someone loses a tag, no problem: that serial number can be removed from the list.

Now, if the tag is implanted in your body, I reasoned, so much the better: it's impossible not to have it when you need it. The RFID tag that makes sense for implantation is embedded in glass and is about the size of a grain of rice. It consists of a microchip and a metal coil, which acts as an antenna. Known as a passive tag, it is an inductive system—that is, a voltage is induced when the coil is in the magnetic field of an RFID reader. Because it's battery-free, a passive tag requires no maintenance.

[Human implantation of RFID tags](#) dates back to at least 1998, when Kevin Warwick, a professor of cybernetics at the University of Reading, in England, implanted an RFID tag above his left elbow, which he used to control doors, lights, and computers around his office. In 2004, VeriChip Corp., in Delray Beach, Fla., had a chip approved for implantation in people. Since then, according to the company, approximately 220 people in the United States (more than 2000 worldwide) have willingly had VeriChip tags implanted into their upper arms. Typically, the implant is used to alert doctors to medical conditions, such as diabetes, if a person is admitted to a hospital unconscious. By scanning the tag, doctors can identify a patient and access personal medical information. There are more frivolous uses, too: some nightclubs have used them to let patrons enter VIP rooms and

bill drinks directly to their accounts.

For my purposes, VeriChip tags had a number of drawbacks. The company requires doctors to register each implantee in a special database. Their tags have a special coating that flesh grows into, locking the tag in place and making its removal difficult and painful. The equipment for reading the tags, priced at around US \$600, is difficult to hack. Additionally, according to approval requirements set up by the U.S. Food and Drug Administration, VeriChip's tags must be implanted in the upper arm, which is awkward to use with door access and other systems—it's a lot easier to open your door or unlock your car by waving your hand rather than by wiggling your bicep.

VeriChip seemed like an awkward option, so I considered animal tags, or "pet chips," which have been around since the late 1980s and which I hoped might be more flexible. Currently, Avid Identification Systems, one of the pioneers in implantable tags, has 19 million to 20 million implanted animals—not including livestock—in its database. Unlike a collar tag, a pet chip is impossible to lose and hard to remove, and it is far less painful for the pet to receive than an ear tattoo.



PHOTO: DAVID STUART

**INDUCTIVE COUPLING:** The author, Amal Graafstra, and his girlfriend, Jennifer Tomblin, have matching RFID implants.

As a human being, I ran into a couple of difficulties with these chips. The companies that sell the chips also require veterinarians to register each pet that receives one, and I didn't want to ask a vet to lie for me. The tags also have the antiremoval coating, and the \$450 tag readers are hard to customize, because they were designed merely with identification, not locks and security, in mind.

Not sure how to proceed, I tried a different tactic and started researching ordinary RFID reader hardware. I found a few devices for \$30 to \$50 that worked with a chip known as the EM4102, which operates at a frequency of 125 kilohertz. I searched for tags to match this hardware and found dozens of them, including access key cards, key-chain tags, and printed-label tags. I also found, to my amazement, glass-ampoule tags costing a few dollars each that looked just like the ones I'd seen for pets, except that these used the EM4102 chip. Bingo! They lacked the antiremoval coating, and I wouldn't have to enter any databases.

The only problem was that they were not sold as implantable tags. After calling the manufacturer, I learned they were not sterile and were typically used in chemical environments or embedded into plastics. The company representative told me that the glass was the same type used on pet tags, but that the EM4102 chip inside was not designed to the standard used for animal tracking. I didn't care about communications standards—I wanted to make sure the glass tag could be safely put into my hand. Figuring that sterilization wouldn't be a difficult challenge, I went online and ordered five of them from Phidgets USA, now Trossen Robotics, a division of Trossen Innovations, Westchester, III.

At this point, I was satisfied with the EM4102, but my girlfriend, Jennifer Tomblin, wasn't convinced that the glass implant wouldn't break in my hand. So on a sunny June day, we decided to experiment. Out in the parking lot of my apartment building, I placed the tag on a piece of wood and tapped it lightly with a hammer. Nothing happened, so I let the hammer fall from a couple of inches above the piece of glass, and that didn't seem to do anything, either. Then I gave it a good whack and promptly pulverized it. We decided that while it was possible to shatter the tag, the blunt force required to do so would also mutilate my hand. In that scenario, a little broken glass would be the least of my worries.

I approached one of my clients, a cosmetic surgeon, to perform the implant. She asked a few basic questions about whether the tag was safe for implantation, and I signed a waiver. The surgeon soaked the glass cylinder in a liquid disinfectant. Because the read range of this tag is only 5 to 7

centimeters, I needed to be able to hold it close to the reader. She made the incision and inserted the tag just underneath the skin. In 5 minutes I had a chip in my left hand, a bandage over the cut, and some grainy cellphone photos to show for it. The soreness from the operation was gone within a few hours. For more details, see sidebar, "How to Get Chipped."

I set to work eliminating keys from my key chain. I had set up one of the RFID readers in my home office for testing, so I picked up the reader and waved it over my hand. The ID number of the chip popped up on my computer screen. I did a little dance, then sat back down and started to work on my home access system. I wanted to configure the reader to unlock the dead bolt on my front door.

I posted the photos of the implant procedure on Flickr.com and sent out an email to some friends and family. Several blogs picked up the story, including BoingBoing.net and Slashdot. I started to receive a flood of questions by e-mail, so I put together a frequently-asked-questions page on my Web site at <http://www.amal.net/rfid.html>.

The messages I received varied in tone from earnest to downright nutty. Some people were curious about how I planned to use the tag; others spouted enraged nonsense about government tracking and mind control. Many wanted to know whether the tags made my hands tingle. If an object taps the skin between my thumb and index fingers, I may feel a slight pinching sensation—but that's about it.

There were e-mails with religious fervor, too. Some Christian groups hold that the Antichrist, sometimes referred to as the beast, will require followers to be branded with a numeric identifier prior to the end of the world—the "mark of the beast." So I got some anxious notes from concerned Christians—including my own mother!

She worried that the implants might one day become some sort of de facto requirement to lead a normal life and to conduct business, much as a driver's license is today. I disagreed with her, arguing that common numeric identifiers like social security numbers and credit cards had initially borne a similar stigma. I pointed out that scarier technologies already exist to identify a person based on facial structure, iris scans, and even scent. [See "RFID Inside," in this issue.]

Implanting people with a foreign device, by contrast, is inherently intrusive and socially difficult to enforce. And implants can be extracted and destroyed—even ones with the so-called antiremoval coating. Should my RFID implants ever be used against me, I'll take them out myself. It'll be about as hard or risky as removing a splinter.

Undeterred by these hypothetical concerns, I continued to rig my life around my new chip. Though I never got rid of my work keys, as was my original intention, I did eliminate most of my personal keys. On weekends, I can go for a walk and not bring keys at all. I close the door behind me, press the "lock" button, and go. When I return, I hold my hand up to the reader and walk in. I also outfitted my 2004 Volkswagen GTI with a reader to unlock the car door and disable the car alarm. I installed another one in my 2005 Suzuki Hayabusa motorcycle so I could hop on, wave my hand, and ride away.

Not long after, Jennifer and I decided to install a reader on her door. I gave her a key card, and I added my ID number to the door's authorized list. Being a gentleman, whenever we reached her apartment door, I'd unlock it for her with my hand.

After a few weeks, she told me she wanted to be able to do that, too. I had a few extra glass tags, so I called my family doctor and scheduled the procedure. Despite a fear of needles—and a brief fainting spell—Jennifer had her hand numbed and the implant injected; 5 minutes later she was ready to swipe open doors herself. I'm pretty sure we are the first couple to get his-and-her RFID implants.

Perhaps a bit belatedly, I began to wonder about the security of these devices and conducted some tests. It turned out that others were also investigating this subject. Jonathan Westhues, a Cambridge, Mass.-based electrical engineer, built an RFID "cloner" device that, when held within inches of the targeted tag, can digitally record and play back the analog radio signal that is emitted by various types of tags, including VeriChip implants and EM4102 tags. A team at Johns Hopkins University, in Baltimore, cracked the encryption used in ExxonMobil's Speedpass, an RFID-based payment system, and then showed how to clone a Speedpass tag and buy gasoline.

I decided to get my second implant, a Philips Hitag 2048 S tag, to address some of my concerns. The \$4 tag, which has 40-bit crypto-security features and 2048 bits of read/write data-storage capacity, was implanted by my family doctor using the same kind of implant needle used with pets, which is basically a syringe loaded with a tag. It operates at 134 kHz and has the same 5-cm read range as the EM4102.

The protected data storage area of this tag holds randomly assigned keys that change each time they are used, so the key can't be easily defeated by cloners. And it can't be decrypted, either—at least not by the Johns Hopkins method, because its encryption is more robust. Another advantage is that the Philips tags are not used in the kinds of business scenarios where attacks are common. My encryption keys are not widely distributed, as they would be for a business, so the attack would have to be targeted directly at me, and attackers would not have the luxury of testing multiple keys. Rather than going to the trouble of chaining together a bunch of field-programmable gate arrays and writing the code to make it all work, as the Johns Hopkins team did, it'd be far easier to just kick in my door.

The only downside to the Hitag is that the reader hardware that supports these enhanced features costs around \$400. The speed at which the tag can be read is slowed down to several times a second by the back-and-forth communication required between the reader and the tag. Compared with the EM4102, which can be read well over 100 times a second, this tag's read speed is glacial, but it is still fine for my needs.

For the time being, this is as far as my RFID lifestyle goes. Since the initial days of my first implant over two years ago, the number of do-it-yourself RFID taggers has grown to include hundreds of people worldwide. While I may want to upgrade one of my implants one day, for now I'm happy to just observe how others develop this trend.

### About the Author

AMAL GRAAFSTRA is an entrepreneur based in Bellingham, Wash. His latest venture is txtGroups, a mobile messaging company. He moderates a forum for RFID hobbyists at <http://www.rfidtoys.net>. His book, RFID Toys, provides step-by-step instructions on how to build RFID projects.

## Sidebar 1

---

### How to Get Chipped



PHOTO: AMAL GRAAFSTRA

Implantation is not for everyone, but if you're determined to do it, here's what I recommend. Before implanting a radio-frequency identification tag in your hand, know how you plan to use it. The tags cost about US \$2 each, but you will spend between \$30 and \$600 for a reader. Remember to factor in the fee for a standard doctor's office visit into your project budget.

Is the extra security of more sophisticated tags, like a Philips Hitag 2048 S, worth the cost of the \$400 RFID readers they work with? Or might simpler readers meet your needs? Check out the RFID implants and implant security forums at <http://tagged.kaos.gen.nz> and at my Web site, <http://www.rfidtoys.net>, to see what others have wanted to know.



PHOTO: AMAL GRAAFSTRA

A simple Web search will turn up links to numerous RFID equipment vendors. Once you've found your tag, buy a couple and test them. Find out from the manufacturer whether your tag is safe for implantation and make sure it works with the reader you choose.

Ready to get implanted? You have two options. A surgical implant takes about 5 minutes, or you can buy an injection kit. The scar from an injection is smaller and heals faster, and the procedure lasts about 30 seconds. I bought my kit from a local pig farmer, but Avid's single-use dispenser kits are available online for \$12 to \$20 apiece. Those come preloaded with an animal implant tag, which you will need to replace. The syringes require a 2- by 12-millimeter tag, so larger tags would have to be inserted surgically.

When you suggest the procedure to your family doctor, be prepared to discuss the safety of RFID tags and offer to sign a liability waiver. If your family doctor is reluctant to do it, ask a cosmetic surgeon. Failing that, if you're really determined, try a body-piercing shop.



PHOTO: AMAL GRAAFSTRA

Once the procedure is about to take place, remember you probably need to sterilize your tag. Don't let your doctor use an autoclave to sterilize the tag, because the heat will destroy it. Soaking it in a liquid disinfectant like alcohol should do the trick.

For tips on how to make your world RFID-accessible, check out my book, *RFID Toys* (John Wiley & Sons, 2006). You can find some free tips on hacking your front door at my Web site. —A.G.