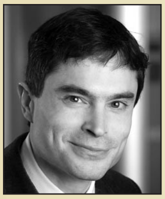
Interview

Editor: Shani Murray ■ smurray@computer.org

An Interview with RFID Security Expert Ari Juels

Tadayoshi Kohno

INTRODUCTION



Ari Juels

In academia and industry, researchers are constantly exploring new uses for RFID tags. Such tags—which wirelessly transmit identification and other information to remote receivers—are already in our library books, car keys, and passports. There are even industry and government proposals for implanting them in humans. Although such RFID implants will enable new applications, they also raise some unique and potentially serious security and privacy concerns.

To help us understand these concerns, I've turned to Ari Juels, chief scientist and director of RSA Laboratories. Juels is a leading expert in computer security in general and in RFID security and privacy in particular. He has chaired or cochaired a number of conferences in the field, and his RFID research has been covered in media outlets such as National Public Radio and the *New York Times*. His innovations in RFID security and privacy also won him a 2004 Technology Review TR100 Young Innovator Award, recognizing him as one of the world's top innovators under the age of 35.

—Tadayoshi Kohno

You were originally trained as a cryptographer, theoretician, and general computer security expert. What made you focus on RFID tags?

It was a 2002 *Economist* article on a proposal to embed RFID tags in Euro banknotes that first stimulated me to think about RFID. ["If Money Could Talk, What Would It Say?" Feb. 2002] It occurred to me that RFID tags might become the ants of the computing world. Individually, ants lead unassuming and uncomplicated lives, but together they constitute the largest biomass on the planet.

RFID security and privacy are also stimulating research topics because the simplest RFID tags—soon to be the most numerous—have such barebones features. Traditional cryptography, a familiar security tool, lies beyond such tags' capabilities. We might wait and hope that Moore's law or advances in lightweight cryptographic primitive design will effect a shift. But in the meantime, we'll have to secure the RFID infrastructure with one hand tied behind our back.

The VeriChip is an RFID chip designed for implantation in humans. Ignoring security and privacy, what could we gain by implanting RFID chips in our bodies?

Tens of millions of house pets already have surgically implanted RFID tags. Thanks to these tags, if an animal turns up at a shelter with a lost collar, we can often still identify it. This is a scenario in which security and privacy are largely uncontroversial, and the benefit of identifying lost animals has prevailed over any objections to the technology.

For people, an analogous situation occurs when first responders encounter confused or unconscious patients. Sometimes these patients lack identifying documents, and as far as I know, first responders are usually prohibited from rifling through patients' pockets owing to safety concerns, such as errant needles. The resulting "John Doe" problem motivates the use of surgically implanted dog tags—which is effectively what VeriChips are (both in the military sense and in their physical similarity to animal implants). The ability to identify a patient and access his or her medical records can have lifesaving consequences.

RFID is also likely to be just one of a panoply of implanted wireless devices. Implanted cardiac defibrillators, insulin pumps, sensors, and other medical devices are very attractive for their minimization of physically invasive interventions.

In your 2006* Journal of the American Medical Informatics Association *paper, why did you argue against using implantable RFIDs, such as the VeriChip, for authentication?

Some applications for implanted RFID tags are ill considered, in my view. One such application is "prosthetic biometrics," or implanted access-

Published by the IEEE CS ■ 1536-1268/08/$25.00 © 2008 IEEE

control or payment cards, if you will. The selling points are that you can't lose these tags and that they overcome some of the unreliability of conventional biometrics. In principle, they can even include cryptographic protections. Some people have proposed implanting such tags in children as a countermeasure to kidnapping—a kind of short-range LoJack.

It takes only a moment's reflection on the combination of, say, an implanted payment or antikidnapping tag and a criminal with a knife to send a shiver down your spine. In 2005, a man with a fingerprint-secured Mercedes lost a piece of his finger to car thieves. With an implanted RFID tag, the situation is in some respects worse. For instance, localizing an implanted tag is, from what I hear, not a straightforward scan-and-remove procedure; it requires surgical exploration.

Is the VeriChip at least reasonably designed for identification—if not authentication—applications?

If you feel comfortable with the attendant privacy risks and the rarity of first responders prepared to read the tags today, then it might be reasonable. The tag is essentially a wireless bar code that broadcasts a unique identifier that can facilitate clandestine tracking. It doesn't broadcast your name, but whenever you identify yourself, you offer an opportunity to bind your name to the tag identifier.

That said, the effective read range for an implanted RFID tag is fairly short—probably on the order of a few feet for a high-powered reader and antenna combination. More important, face recognition, location-based mobile-phone services, and the chattering constellation of personal wireless devices that more and more people are carrying will probably overshadow concerns about RFID-based tracking.

Do implanted RFID tags pose any other security problems?

There's another risk, much more fanciful at this point, but worth thinking about as designs evolve. To prevent tracking, an RFID tag can't, of course, broadcast a static identifier. Instead, it must emit a changing, cryptographically protected identifier.

But if you have a wireless identification device implanted in your body, and it's emitting cryptographically protected values, how do you know that all it's doing is identifying you? How do you know it's not acting as a sensor and secretly reporting medical information to your employer ("Yoshi isn't getting much exercise") or recording and relaying RFID-reader events ("Yoshi has been to a casino today")? This problem of "covert channels" is challenging.

What can we do to prevent or detect covert channels?

It's a labyrinthine problem. You can give the implanted device's owner a secret key—the ability, essentially, to decrypt the values the tag outputs. But forcing people to manage these keys would be a sticky business. I've got enough problems with my email passwords. I don't want to manage "body" passwords too!

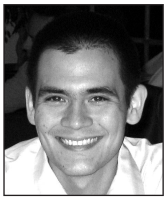
We might then ask, is there some open, public way to audit implanted RFID tags to ensure that they're only emitting identifiers? In a recent paper, some colleagues and I showed that such auditing is at odds with strong privacy ["Covert Channels in Privacy-Preserving Identification Systems," 2007, www.rsa.com/rsalabs/node.asp?id=3358]. You can't have both in the same device. The ability to audit actually means an ability to track. This impasse isn't a dead end, though; some compromises are possible.

Still, there are other twists. How do I know that my device isn't simply transmitting at some secret frequency? How do I know that it doesn't behave correctly when I'm watching it but release information when it receives a special password? To resolve these problems, it would be necessary to audit reader emissions and a broad range of frequencies, to play a spectral game of cat and mouse.

Do you have any closing thoughts on RFID security and privacy in particular or implantable electronics in general?

Much of the discourse around—and research on—technical solutions to RFID security and privacy problems seems to center on cryptographic primitives and protocols. It's often intimated that encryption, once it percolates down into small computing devices, will provide good solutions.

Historically, though, key management has often proven to be the rock on which the best computer-security designs have foundered. I expect RFID and implantable wireless devices to recapitulate this lesson with new twists. RFID tags, unlike laptops, for instance, can change ownership many times over their lifetimes, often across organizations in unpredictable ways. A case containing bottles of medication typically wends its way thousands of miles and through the hands of several corporations. How can we ensure that the PINs or keys that secure RFID tags closely follow such convoluted trajectories of possession? And how can we ensure, similarly, that medical implants are well protected against mistaken or malicious manipulation but freely accessible to medical personnel in emergencies? Key management is a truly knotty problem at the heart of the challenges of security and privacy—a problem that is all too easy to overlook but that pervasive wireless devices will illuminate and amplify. P



Tadayoshi Kohno is an assistant professor in the University of Washington's Department of Computer Science and Engineering. Contact him at yoshi@cs.washington.edu.