

Tag Implants May Be Dangerous for Security Apps, Says Group

Because VeriChip's tag is easily copied, a technologist group claims it is a poor choice for authenticating the bearer's identity. But VeriChip says its tags should be combined with other authenticators.

By Mary Catherine O'Connor

Aug. 22, 2006—An implantable passive RFID tag made by the [VeriChip Corp.](#) can be cloned and is, therefore, not an appropriate device for use in building access control, says an article in an upcoming issue of the [Journal for American Medical Informatics Association](#) (JAMIA). VeriChip's tag, approved by the [Food and Drug Administration](#) (FDA) for human implantation, consists of a low-frequency inlay enclosed in a rice-sized glass capsule. VeriChip sells it for two different applications: VeriMed, which uses the tag to identify patients and access their medical records in the event of an emergency, and VeriGuard, which utilizes the tags to identify people for the purposes of granting or denying access to buildings and offices.

"I'd suspected for some time that the VeriChip was susceptible to cloning attacks," says Ari Juels, manager and principal research scientist for [RSA Laboratories](#), a provider of digital security products. His suspicions were confirmed early this year after he met with a computer scientist, [Jonathan Westhues](#), who, weeks earlier, had cloned the VeriChip tag implanted in the arm of technology journalist [Annalee Newitz](#). Juels and Westhues are two of the JAMIA article's four authors, along with John Halamka, CIO of [Beth Israel Deaconess Medical Center](#), which offers the VeriMed system, and Adam Stubblefield, a [Johns Hopkins University](#) faculty member studying RFID security. Halamka also has the VeriChip implant and is a subscriber to the VeriMed system.

Westhues used a cloner he created, and which Juels describes as a kind of RF tape recorder, to capture the RF signal transmitted by a passive VeriChip tag read. He then replayed that same signal (without even having to convert it to the digits encoded to it) to another interrogator, which read the signal from the cloner just as it would from a tag. This is possible because VeriChip does not use any data encryption to protect the 16-digit number it encodes to the tags it sells.

In the paper, the authors posit that VeriChip tags "should serve exclusively for identification, and not authentication or access control" because the ease with which the tags can be cloned leaves any security system built on the VeriChip IDs highly vulnerable to attacks.

VeriChip says its implantable tag uses an [ISO](#) air-interface protocol, though the company could not supply *RFID Journal* the specific ISO standard it follows.

Westhues' cloner device can also act as an RFID interrogator—but not one sophisticated enough to clone (or "spooft") tags protected through encryption or a challenge-response protocol requiring the interrogator to send a password before the tag responds with its data. Nonetheless, Juels says, it is small and effective enough that a nefarious party could conceivably use it to read a tag embedded in the arm of a subway rider. If that

VeriChip customer had the implant purely to be identified in a medical database in the case of an emergency, reading and cloning the VeriChip's ID would not provide any benefit to the attacker—unless that attacker had an interest in accessing the rider's medical history and the ability to access the secure VeriMed database.

To access this medical information, an attacker would need a URL for the Web-based database, as well as a valid log-in name and password. As a security measure, VeriChip automatically sends an e-mail message to the bearer of the implant each time his or her account is accessed, along with the name of the facility linked to the password used to log on to the account.

If a VeriChip customer, however, had the implant for the purpose of entering his secure office building—by holding the arm with the implant within inches of an access-control reader at the building's entrance—then the ability to clone the number could certainly have value to the attacker.

Nonetheless, Juels and his coauthors are not recommending that VeriChip add a level of data security to its tags. Making the tags more secure would put people who use the implants for building access control—such as three employees of Citywatcher.com, a video surveillance company in Ohio—in danger.

"An attacker can readily seize and use a physically transferable authenticator, such as an ATM card, without seizing its owner," says the paper. Although an attacker currently would be able to use Westhues' cloner or a similar device to clone a VeriChip tag's ID, this would not be true if the company changed its tags to make cloning impossible, or nearly impossible. The paper goes on to note that in 2005, thieves in Malaysia once severed the finger of a man to steal his Mercedes, which had a biometric security system and would run only after scanning the driver's fingerprint. What, the authors pose, if thieves tried to extract an implanted VeriChip tag in order to access a building?

"Somewhat paradoxically," the paper concludes, "we maintain that a VeriChip should be vulnerable to spoofing by design, to discourage physical attacks on VeriChip bearers." It maintains, furthermore, that VeriChip implants should not be used to authenticate—that is, to *prove* the identity of those with the implants—but, rather, just to identify them. A security system using the implants, therefore, would need some other type of authenticating factor.

VeriChip's vice president for medical applications, Richard Seelig, says the article is based on false assumptions. "VeriGuard is meant to enhance current [security] measures rather than to replace them," he says. "That's why the paper's hypothesis is made in a vacuum. In the real world, experts always recommend having at least two means of identification to enter secured locations."

Seelig claims he's not sure whether Citywatcher.com is using VeriGuard as a standalone system or in combination with another security system that would require a second means of authentication. Still, he says, "I certainly hope that [VeriGuard] is being deployed with other forms of ID and authentication." Citywatcher.com did not respond to a request for an interview as of press time.

Seelig says he also thinks it would have made more sense for the group that wrote the paper to test some of the scenarios they describe in the paper, such as secretly reading a person's VeriChip implant while on a subway train. Halamka has the implant, he notes, and could have ridden in a subway train with Westhues and his cloner. Without having performed such an experiment, Seelig says, the paper is based purely on assumptions.

The article's authors note that they are not attempting to make any "categorical judgment as to whether or not VeriChip implantation is beneficial." In fact, Beth Israel Deaconess Medical Center is equipped with VeriChip interrogators and can access the VeriMed database to retrieve the medical records of people with implants. However, they do say they are trying to encourage the kind of scrutiny of the implants that led them

to write the paper.

An electronic version of the JAMIA article on VeriChip will be available later this month on the publication's Web site (nonsubscribers can read an abstract of the paper, or pay a \$5 fee to read the complete article). It will also be published in the November/December issue of the magazine.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved