



Computer Crime Research Center

Security Gets Under Your Skin

Date: **March 04, 2005**

Source: [Computer Crime Research Center](#)

By: CCRC staff

Joseph Krull, former intelligence officer and present security expert for Virtual Corporation, recently let VeriChip implant a small RFID chip under the skin of his right arm.

VeriChip, a company that produces automatic identification ware for identifying pets, livestock and food products -- and humans seem to be its next market.

High-profile human implants began in July, when attorney general of Mexico Rafael Macedo de la Concha and 15 other Mexican security officials agreed to chip implants to act as access control to secure areas of their headquarters.

In December, John D. Halamka, the CIO of Harvard Medical School, also got chipped, saying he wanted to experience the process for himself. According to a VeriChip press release, Halamka reported that he was able to climb Mount Washington without any ill effects from the chip. He thinks the technology could be used to identify unconscious patients, matching hospital patients to the correct meds and verifying that patients were medicated.

Krull leads the information security practice of Virtual Corporation, a consulting company that consults on business continuity, information security and supply chain management. He's been a senior security executive at Telecom Finland, Philips Electronics and Lucent Technologies and was a senior intelligence and security officer with the U.S. Defense Intelligence Agency at American embassies overseas from 1979 to 1996.

You would ask how to get "chipped"? He saw a presentation on the chip at a European conference on privacy and identification in 2003.

He made my own risk analysis, uploaded his blood type, allergies, business card, next of kin. He has a specific medical condition -- there's a metal plate under his eye. He has been told by doctors many times that if he was incapacitated, doctors would assume he had a head injury, and their first course of action is to start drilling holes. If he has a chip

and a reader they can scan him.

There's a secure Web site where he -- and only he -- can change his data. It's strictly self-service. If he can control what data goes in and gets added and subtracted, he's fine. If he had a health condition, for example, that might deter employers, he wouldn't put it in the database. But the minute it becomes mandatory or gets combined with other data, the chip is coming out.

If you compromise a biometric feature, it's gone forever, Joseph Krull says. "This is a replicable biometric. You need three things to get to my information: a reader, being within 2.5 inches of my arm, and the password or PIN code for my database. If managed correctly, it can be a great technology from the security point of view," he adds.