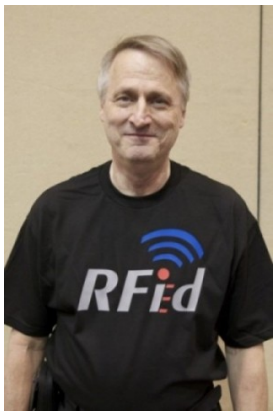
Source: http://www.wired.com/threatlevel/2009/08/fed-rfid/#ixzz0eOg6C98M

Feds at DefCon Alarmed After RFIDs Scanned

By Kim Zetter
August 4, 2009



LAS VEGAS — It's one of the most hostile hacker environments in the country –- the DefCon hacker conference held every summer in Las Vegas.

But despite the fact that attendees know they should take precautions to protect their data, federal agents at the conference got a scare on Friday when they were told they might have been caught in the sights of an RFID reader.

The reader, connected to a web camera, sniffed data from RFID-enabled ID cards and other documents carried by attendees in pockets and backpacks as they passed a table where the equipment was stationed in full view.

It was part of a security-awareness project set up by a group of security researchers and consultants to **highlight privacy issues around RFID.** When the reader caught an RFID chip in its sights — embedded in a company or government agency access card, for example — it grabbed data from the card, and the camera snapped the card holder's picture.

But the device, which had a read range of 2 to 3 feet, caught only five people carrying RFID cards before Feds attending the conference got wind of the project and were concerned they might have been scanned.

Kevin Manson, a former senior instructor at the Federal Law Enforcement Training Center in Florida, was sitting on the "Meet the Fed" panel when a DefCon staffer known as "Priest," who prefers not to be identified by his real name, entered the room and told panelists about the reader.

"I saw a few jaws drop when he said that," Manson told Threat Level.

“There was a lot of surprise,” Priest says. “It really was a ‘holy shit,’ we didn’t think about that [moment].”

Law enforcement and intelligence agents attend DefCon each year to garner intelligence about the latest cyber vulnerabilities and the hackers who exploit them. Some attend under their real name and affiliation, but many attend undercover.

Although corporate- and government-issued ID cards embedded with RFID chips don’t reveal a card holder’s name or company — the chip stores only a site number and unique ID number tied to a company or agency’s database where the card holder’s details are stored — it’s not impossible to deduce the company or agency from the site number. It’s possible the researchers might also have been able to identify a Fed through the photo snapped with the captured card data or through information stored on other RFID-embedded documents in his wallet. For example, badges issued to attendees at the Black Hat conference that preceded DefCon in Las Vegas were embedded with RFID chips that contained the attendee’s name and affiliation. Many of the same people attended both conferences, and some still had their Black Hat cards with them at DefCon.

But an attacker wouldn’t need the name of a card holder to cause harm. In the case of employee access cards, a chip that contained only the employee’s card number could still be cloned to allow someone to impersonate the employee and gain access to his company or government office without knowing the employee’s name.

Since employee access card numbers are generally sequential, Priest says an attacker could simply change a few digits on his cloned card to find the number of a random employee who might have higher access privileges in a facility.

“I can also make an educated guess as to what the administrator or ‘root’ cards are,” Priest says. “Usually the first card assigned out is the test card; the test card usually has access to all the doors. That’s a big threat, and that’s something [that government agencies] have actually got to address.”"

In some organizations, RFID cards aren’t just for entering doors; they’re also used to access computers. And in the case of RFID-enabled credit cards, RFID researcher Chris Paget, who gave a talk at DefCon, says the chips contain all the information someone needs to clone the card and make fraudulent charges on it — the account number, expiration date, CVV2 security code and, in the case of some older cards, the card holder’s name.

The Meet-the-Fed panel, an annual event at DefCon, presented a target-rich environment for anyone who might have wanted to scan government RFID documents for nefarious purposes. The 22 panelists included top cybercops and officials from the FBI, Secret Service, National Security Agency, Department of Homeland Security, Defense Department, Treasury Department and U. S. Postal Inspection. And these were just the Feds who weren’t undercover.

It's not known if any Feds were caught by the reader. The group that set it up never looked closely at the captured data before it was destroyed. Priest told Threat Level that one person caught by the camera resembled a Fed he knew, but he couldn't positively identify him.

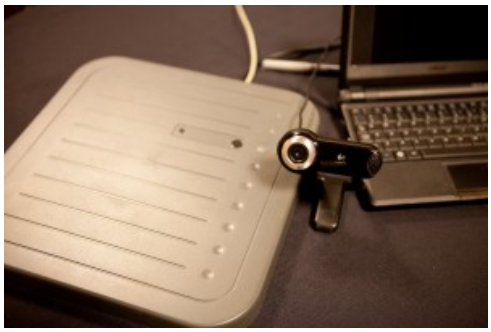
"But it was enough for me to be concerned," he said. "There were people here who were not supposed to be identified for what they were doing … I was [concerned] that people who didn't want to be photographed were photographed."

Priest asked Adam Laurie, one of the researchers behind the project, to "please do the right thing," and Laurie removed the SD card that stored the data and smashed it. Laurie, who is known as "Major Malfunction" in the hacker community, then briefed some of the Feds on the capabilities of the RFID reader and what it collected.

The RFID project was a collaboration between Laurie and Zac Franken — co-directors of Aperture Labs in Great Britain and the ones who wrote the software for capturing the RFID data and supplied the hardware — and Aries Security, which conducts security-risk assessments and runs DefCon's annual Wall of Sheep project with other volunteers.

Each year the Wall of Sheep volunteers sniff DefCon's wireless network for unencrypted passwords and other data attendees send in the clear and project the IP addresses, login names and truncated versions of the passwords onto a conference wall to raise awareness about information security.

This year they planned to add data collected from the RFID reader and camera (below) — to raise awareness about a privacy threat that's becoming increasingly prevalent as RFID chips are embedded into credit cards, employee access cards, state driver's licenses, passports and other documents.



Brian Markus, CEO of Aries Security who is known in the hacker community as "Riverside," said they planned to blur the camera images and superimpose a sheep's head over faces to protect identities before putting them on the wall.

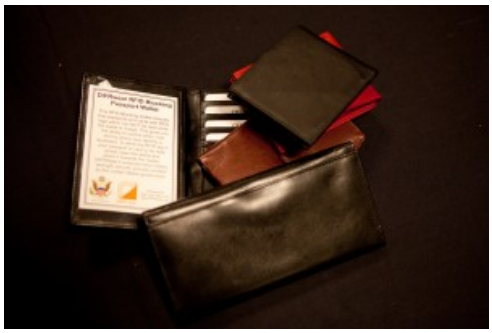
"We're not here to gather the data and do bad things with it," he said, noting that theirs likely wasn't the only reader collecting data from chips.

"There are people walking around the entire conference, all over the place, with RFID readers [in backpacks]," he says. "For $30 to $50, the common, average person can put [a portable

RFID-reading kit] together…. This is why we're so adamant about making people aware this is very dangerous. If you don't protect yourself, you're potentially exposing your entire [company or agency] to all sorts of risk."

In this sense, any place can become a hostile hacker environment like DefCon, since an attacker with a portable reader in a backpack can scan cards at hotels, malls, restaurants and subways, too. A more targeted attack could involve someone simply positioned outside a specific company or federal facility, scanning employees as they entered and left and cloning the cards. Or someone could even wire a coil around a door frame to collect data as people pass through the door, which Paget demonstrated at DefCon.

"It takes a few milliseconds to read [a chip] and, depending on what equipment I've got, doing the cloning can take a minute," says Laurie. "I could literally do it on the fly."



Paget announced during his DefCon talk that his security consulting company, H4rdw4re, will be releasing a $50 kit at the end of August that will make reading 125-kHz RFID chips — the kind embedded in employee access cards — trivial. It will include open source software for reading, storing and re-transmitting card data and will also include a software tool to decode the RFID encryption used in car keys for Toyota, BMW and Lexus models. This would allow an attacker to scan an unsuspecting car-owner's key, decrypt the data and open the car. He told Threat Level they're aiming to achieve a reading range of 12 to 18 inches with the kit.

"I often ask people if they have an RFID card and half the people emphatically say no I do not," says Paget. "And then they pull out the cards to prove it and … there has been an RFID in their wallet. This stuff is being deployed without people knowing it."

To help prevent surreptitious readers from siphoning RFID data, a company named DIFRWear was doing brisk business at DefCon selling leather Faraday-shielded wallets and passport holders (pictured above right) lined with material that prevents readers from sniffing RFID chips in proximity cards.

(Dave Bullock contributed some reporting to this piece.)
Photo at top: Former Fed Kevin Manson got RFID'd at DefCon and all he got was this spoof t-shirt — made by Brian Markus. All photos by Dave Bullock.

See also: A Hacker Games the Hotel Open Sesame: Access Control Hack Unlocks DoorsScan This Guy's Passport and Watch Your System Crash