Snowed Under By Security Challenges

blog.atlasrfidstore.com/rfid-security-banking

Laurie Wiegler

July 18, 2014

In the U.S., credit cards are not yet as secure as they could be. For all intents and purposes, the standard debit or credit card may employ a rudimentary form of NFC, but the infrastructure to support its pervasive use isn't ubiquitous. And not all cards here are wireless, either.

Europe is more advanced than the U.S., according to some experts, because of the use of wireless technology to help secure each transaction.

Other security concerns abound including identify theft, hacking, and so forth, and all require some kind of stopgap to address the breach.

As was reported in the story *RFIDinsider* published on security at the Sochi Olympics , for example, even access badges to athletic games sport an RFID chip. And at the Games, or anywhere technology exists — from a NASA vessel to your smartphone — trust that someone, somewhere is trying to break in.

Contactless cards present challenges

"A contactless card is, for all practical purposes, like NFC," explains Victor Vega, director of RFID/NFC Solutions and Marketing at NXP. "So the more secure credit cards are contactless."

If it's contactless, it's similar to using HF or NFC, he says, in which there's a coil and a chip with security inside. So, if one looks at the [European and some other players in the] banking industry, for example, its wireless technology is "basically an NFC type of card". Varying levels of encryption sophistication can be used on these cards, he adds.

So, are Americans at big risk of credit card fraud?

"Yes, people are at risk," Vega says. "Fraud has become a bigger and bigger problem, and the liability falls on the hands of either the retailer — because they have to spend more money for a transaction — or the bank, because they must absorb it [the cost]."

By 2015, Vega says, banks here in the States will be mandated to use wireless technology on all debit and credit cards issued which should, theoretically at least, help limit fraud.

Victor Vega serves as the NFC / RFID Solutions Director for NXP Semiconductors.

What Can Go Wrong

Vega cites the unfortunate example of a colleague who was the victim of credit card fraud. The perpetrator opened numerous fraudulent accounts under this coworker's name, exploiting the lack of pervasive wireless technology in the U.S.

The imbroglio started with the impression of this individual's VISA card.

"Someone got ahold of that, and his address, when he applied for a mortgage loan. [Then the thief obtained] every bit of information and they started opening up new accounts, like if you go to Macy's and get a 25 percent discount. [This individual] used [my colleague's] credit card and opened a ton [of new accounts]."

If one wonders if her debit card is secure, check for the wireless waves on the logo, he says. For example, British-based bank Barclays issues a wireless card, as shown below.

Example of a contactless credit card

Other (In)security Issues at Play

Of course, a credit or debit card isn't the only point of concern for those of us looking to secure our digital footprint. Writers, lawyers, doctors, and your average teenage texter, all have a lot to be concerned about.

Edward Snowden brought much of this to light, and whatever your opinion about him – traitor, hero or somewhere in between – everyone agrees he's furthered the discussion about security breaches.

On one's laptop or iPhone, or any other type of device, RFID is helping secure our transactions. Take, for example, getting a passport. At the time this reporter's was issued in 2005, no RFID chip was added. Now all of that has changed, as we reported on *RFIDinsider* a few months ago.

Pankaj Rohatgi, an engineer with San Francisco-based Cryptography Research, a division of Rambus, says, "In the RFID space, [encryption works to] create data and secure it so only the intended recipients can see it. If you are transmitting some personal information about a user from an RFID tag to a reader, you don't want someone to see that so they can replicate that."

Encryption began to ramp up in popularity a few years ago, and no doubt even more so since the Snowden NSA revelations.

In simplest terms, says Rohatgi, "Cryptography is a mathematical technique that is used to create secret messages and to verify messages which are secret."

With millions of devices in use every day, it’s imperative that cryptography is implemented securely.

Pankaj Rohatgi with San Francisco-based Cryptography Research

RFID didn’t used to care

Like all new technologies, its surrounding uses and impetuses evolve over time.

Rohatgi points out that at the dawn of RFID a decade ago, most were just concerned with tracking-for-inventory, or at least mainly. All of that has changed. Now everyone who pays to chip his tomatoes or hospital employee badges wants to make sure unscrupulous individuals aren’t exploiting the technology.

Luckily, the brains behind RFID security aren’t getting any duller.

Cryptography research is a keen example of how RFID is being secured, and other methods are also at play, such as phasing in wireless technology on our debit cards.

“Yes, people [hackers] could figure out what the tag [number] is, ‘listen’ to the tag and clone it”, says Rohatgi. “People start attacking the keys, and that is where we come in.”

He likes to think they’ve found a solution, though.

“We specialize in techniques so secret cryptographic keys remain secret,” he says.

Top Ten Security Tips from Bill Carey, VP of Marketing for password management firm RoboForm

1. Regularly update software to eliminate security weaknesses. Windows, Macs, and all browsers regularly provide free software updates; take advantage of this to close security loopholes.
2. When you’re done with using a website, log off and close your browser. This will prevent others from gaining access to your account.
3. Create passwords with combinations of upper and lowercase letters, numbers and special characters.
4. Don’t use personal information in your password, such as your name, your partner’s name, your child’s name, your occupation, telephone number, birth date, etc.
5. Small businesses have to hold their employees accountable for their security. Employees must adopt safe security habits to keep their information and the company’s information protected. Consider putting a formal cyber-security policy into effect.
6. Make sure that you use a PIN or #password on your mobile phone.
7. Use the ‘Keystroke’ method for making passwords. Choose a password and create a keyboard mapping system. One key to the left and one up would make the password “tinmen” change to “47gh2g”
8. Disable pictures on your e-mail and read it in plain text. The sender will not be able to identify if you’ve opened the e-mail.
9. Don’t keep a record or list of your passwords in unencrypted files on your computer or phone.
10. Have a disposable e-mail address. Only give your actual e-mail address out to who people who need it. This will avoid mass spam and keep your inbox clean.