The Media and RFID

I recently traded in my 12-year-old Subaru Outback and purchased a pre-owned Infiniti Q50. The car, like many recent models, uses RFID to recognize a fob that you can leave in your pocket or purse. You simply press a button on the dashboard, and if the correct RFID-enabled device is present, the car starts.

The system also works outside the car, within three feet (one meter) or so. This conveniently allows you to simply open a locked car door or trunk (also known as the boot) when the fob is present. And you can lock all the doors or open all the doors with a push of a button on the door handle.

I bring this up not because my car is unique. Far from it. This technology is being used in more and more new models. I bring it up because it strikes me as odd that journalists have not questioned the security of these systems, but they did question a similar system used in credit cards.

Let me explain. The way these key fobs work is there is a unique ID stored inside the RFID transponder that a reader inside the car must receive. But the reader also sends a new code to the transponder each time the fob is used. The next time you want to start the car, the reader must match both codes—the static ID and the dynamic serial number sent by the reader—before the car will start.

The dynamic code makes the system extremely secure. Even if thieves could clone the transponder in your key fob, it would be hard for them to know the specific code the reader sent to the transponder. And that's why few cars have been stolen by people hacking the RFID-enabled ignition system.

RFID-enabled credit cards used a similar system. In addition to matching the serial number in the transponder, the card reader also had to read a dynamic credit verification value (CVV). Magstripe cards use only a static CVV printed on the back of the card. So if someone stole the ID in your credit card and capture your name and account number, they would not be able to create a clone because when you use the real card the dynamic CVV would change (see Are RFID-Enabled Credit Cards Safer Than Magstripe Cards?).

No system is 100 percent secure, but RFID key fobs are more secure than physical keys because any time you hand over your

key to a parking lot attendant or a valet at a restaurant or hotel, that key can be copied. The RFID ignition device is like a key that changes each time it's used so it cannot be copied.

I'm not sure why the media ran so many negative articles about RFID-enabled credit cards (see L.A. Broadcaster Misinforms Public About RFID Credit Cards and ABC Eyewitness News Presents Selective Facts About RFID Credit Cards), but there have been few scare stories about RFID in cars. Perhaps the media senses people feel inherently vulnerable when using credit cards. Perhaps RFID is better-known now so journalists trust it more. Whatever the reason, I am glad that we have not seen the type of misleading articles that led most credit card companies to abandon RFID.

Mark Roberti is the founder and editor of RFID Journal. *If you would like to comment on this article, click on the link below. To read more of Mark's opinions, visit the RFID Journal Blog, the Editor's Note archive or RFID Connect.*