The ID Chip You Don't Want in Your Passport

By Bruce Schneier

The Washington Post
Saturday, September 16, 2006; A21

If you have a passport, now is the time to renew it -- even if it's not set to expire anytime soon. If you don't have a passport and think you might need one, now is the time to get it. In many countries, including the United States, passports will soon be equipped with RFID chips. And you don't want one of these chips in your passport.

RFID stands for "radio-frequency identification." Passports with RFID chips store an electronic copy of the passport information: your name, a digitized picture, etc. And in the future, the chip might store fingerprints or digital visas from various countries.

By itself, this is no problem. But RFID chips don't have to be plugged in to a reader to operate. Like the chips used for automatic toll collection on roads or automatic fare collection on subways, these chips operate via proximity. The risk to you is the possibility of surreptitious access: Your passport information might be read without your knowledge or consent by a government trying to track your movements, a criminal trying to steal your identity or someone just curious about your citizenship.

At first the State Department belittled those risks, but in response to criticism from experts it has implemented some security features. Passports will come with a shielded cover, making it much harder to read the chip when the passport is closed. And there are now access-control and encryption mechanisms, making it much harder for an unauthorized reader to collect, understand and alter the data.

Although those measures help, they don't go far enough. The shielding does no good when the passport is open. Travel abroad and you'll notice how often you have to show your passport: at hotels, banks, Internet cafes. Anyone intent on harvesting passport data could set up a reader at one of those places. And although the State Department insists that the chip can be read only by a reader that is inches away, the chips have been read from many feet away.

The other security mechanisms are also vulnerable, and several security researchers have already discovered flaws. One found that he could identify individual chips via unique characteristics of the radio transmissions. Another successfully cloned a chip. The State Department called this a "meaningless stunt," pointing out that the researcher could not read or change the data. But the researcher spent only two weeks trying; the security of your passport has to be strong enough to last 10 years.

This is perhaps the greatest risk. The security mechanisms on your passport chip have to last the lifetime of your passport. It is as ridiculous to think that passport security will remain secure for that long as it would be to think that you won't see another security

update for Microsoft Windows in that time. Improvements in antenna technology will certainly increase the distance at which they can be read and might even allow unauthorized readers to penetrate the shielding.

Whatever happens, if you have a passport with an RFID chip, you're stuck. Although popping your passport in the microwave will disable the chip, the shielding will cause all kinds of sparking. And although the United States has said that a nonworking chip will not invalidate a passport, it is unclear if one with a deliberately damaged chip will be honored.

The Colorado passport office is already issuing RFID passports, and the State Department expects all U.S. passport offices to be doing so by the end of the year. Many other countries are in the process of changing over. So get a passport before it's too late. With your new passport you can wait another 10 years for an RFID passport, when the technology will be more mature, when we will have a better understanding of the security risks and when there will be other technologies we can use to cut the risks. You don't want to be a guinea pig on this one.

Bruce Schneier writes often on security subjects.