itbusiness.ca
Business Advantage through Technology

Print

Experts question security of Canada's e-passports

The government began issuing e-passports in January this year in a bid to cut the circulation of counterfeit passports and secure our borders. However, some security experts worry the technology could expose users to more risks.

10/19/2009 7:42:00 AM
by Nestor E. Arellano

E-passports – which Canada began issuing in January this year – could expose users to data theft and other privacy issues, security experts say.

Canada's e-passports are part of a global effort to establish a more secure form of identification for travelers.

But some security experts are worried there may be several weaknesses in the system.

The move to replace existing travel documents with passports that are embedded with RFID (radio frequency identification) chips containing the bearer's personal data is intended to cut down passport forgery and strengthen international border security.

Full implementation is set for 2011, according Leslie Crone, director of international programs for Passport Canada.

The new passports will enable customs officers to verify passport information with the use of RFID readers, said Crone.

See related story

Ontario's new RFID driver's license still has privacy flaws, commissioner says

Governments, however, are not adequately informing individuals about security risks inherent in most e-passport systems, says one security researcher.

"Very often governments are keen on selling technologies as secure even if they are not. E-passports are an excellent example of this," says Adam Laurie, freelance security researcher.

Laurie, also known as Major Malfunction, is a penetration testing expert who is also widely credited for cracking the code and breaking into the data held inside music CDs when the disks were made commercially available and thought to be secure in the 1980s.

He recently spoke at the Security Conference Toronto (SecTor) held in the city earlier this month.

Although e-passports may vary from country to country, many share some common weaknesses, according to Laurie.

For one, he said, the key to the RFID chip can be plainly seen printed on the passports themselves. "Often the code is based on the passport holder's birthday, country of origin and other pieces of information, printed in sequence on the passport itself."

During his presentation, Laurie also demonstrated how a software toolkit developed by Dutch security researcher Jeroen van Beek from the University of Amsterdam, can be used to create an RFID chip encoded with altered data from his son's British e-passport.

Laurie took a writeable RFID chip, loaded it with data (name, birth date, photo, etc) taken from his son's passport, then hashed that data and made a self-signed certificate using the same parameters of a legitimate passport signature so that passport readers would accept it as legitimate.

"This means I can now become my own passport issuing country," the researcher said.

Theoretically, Laurie said, the RFID chip with the altered data can be switched for the one on his son's passport.

If Laurie ever decides to do just that, when the travel document is scanned at an airport it will reveal the photo not of a teenaged boy but that of the world's most wanted terrorist – Osama Bin Laden.

But there is a system designed to expose a fake chip.

The International Civil Aviation Organization (ICAO), the United Nations body that established the standards for e-passports, set up a Public Key Directory (PKD). The PKD contains the signature codes of each of the 45 countries that issue e-passports.

Under this system, a passport reader at a Canadian airport could instantly check the database to determine if the signature in a U.S. passport matches the signature provided to the PKD by the U.S.

But this failsafe feature has it own pitfall, according to Laurie.

"Only five of the 45 issuing countries (Australia, New Zealand, Japan and the U.S) are using the PKD to check RFID signatures on e-passports," he said.

"The whole thing is based on a backend check of the database. With an incomplete database, the whole thing falls apart," said Laurie.

Anticipating chip cloning, the ICAO also developed an active authentication measure for e-passports, according to Dutch researcher Van Beek.

But active authentication is optional and only 20 to 25 per cent of the 45 countries issuing are using it, Van Beek said. Other researchers worry that bearers of RFID tagged documents may be exposed to unauthorized scanning of their personal data.

The total market for hardware, software and services providing e-ID documents will reach US$1 billion by 2012 while the total market for contactless e-passports alone is set to grow by nearly $300 million by that year, according to study from New York-based ABI Research.

Despite this growth, however, a senior analyst with the firm said RFID technology is not ideal for storing personal data.

"RFID technology is ill-suited to the tagging of secure documents," said Jonathan Collin, senior analyst for ABI Research.

Privacy concerns abound over the possibility that data contained in the documents might be read from a distance by "eavesdroppers" equipped with RFID readers.

RFID technology "is likely to create concerns among citizens, given the greater read-range of the technology compared with high-frequency transponders," Collins said.

Crone from Passport Canada, however, said that Canadian e-passports are different from enhanced driver licenses (EDL).

Beginning June 1 this year, American travelers returning from Canada, Mexico, Bermuda and the Caribbean by land and by sea borders, are required to show U.S. border guards a valid passport, an e-passport or RFID-enabled EDLs.

RFID scanners can read EDLs from a distance of 100 feet. "E-passport chips must be read within 10 centimeters, which makes eavesdropping practically impossible, said Crone.

E-passports also give out a "pseudo-unique ID" which changes each time an e-passport is scanned as a further deterrent to eavesdropping, according to Laurie.

Still, the security researcher manages to dish out one more chilling scenario.

While eavesdropping tools are not able to read from a distance the personal data within e-passports, they are able to identify passport's country of origin. This could make it easier for some groups to target individuals of certain nationality, says Laurie.

"It would not be difficult for certain groups set a bomb to detonate when an RFID reader attached to the explosive senses that a desired number of individuals carrying passports from a target country are in the vicinity," he said.

Print

Close Window