Researchers uncover privacy flaw in e-passports

September 26 2019

Credit: CC0 Public Domain

Researchers at the University of Luxembourg have discovered a flaw in the security standard of biometric e-passports that has been used worldwide since 2004. This standard, ICAO 9303, allows e-passport readers at airports to scan the chip inside a passport and identify the holder.

Most passports today use the standard ICAO 9303, which is issued by the International Civil Aviation Organization (ICAO). The standard is designed to ensure that the privacy and unlinkability of the passport holder is protected to the highest degree. Unlinkability ensures that an attacker could not distinguish if two elements are closely related.

Dr. Ross Horne, Prof. Sjouke Mauw, Ph.D. candidate Zach Smith and Master student Ihor Filimonov tested the standard. They discovered a flaw that allows specific non-authorized equipment to access passport data. "With the right device, you can scan passports in close vicinity and re-identify previously observed passport holders, keeping track of their movements," Dr. Horne explains. "Thus, passport holders are not protected against having their movements traced by an unauthorized observer."

Limits and implications of the flaw

An unauthorized device scanning a passport within several meters can identify and keep track of that passport, even though it cannot read the passport. Thus, the privacy of the passport holder are vulnerable to potential attacks, even though the flaw does not allow attackers to read all information from a given passport or to compromise biometric information stored in a chip inside the passport.

"As most passports today use the same standard, this security flaw potentially has global impact," continues Dr. Horne. In Europe, such a security breach likely violates requirements from the EU data protection framework. Governments have the responsibility to protect individual privacy and to ensure that official documents are bulletproof against such attacks.

The team of researchers shared their test results with ICAO in June 2019. They also outlined several approaches for restoring privacy protection, based on the assumption that the manufacturers of e-passport readers must take responsibility for ensuring privacy protection of passport holders.

The results of the study, "Breaking Unlinkability of the ICAO 9303 Standard for e-Passports Using Bisimilarity," were presented on Tuesday 24 September at ESORICS 2019, a high-level systems security conference in Europe.

More information: Ihor Filimonov et al, Breaking Unlinkability of the ICAO 9303 Standard for e-Passports Using Bisimilarity, *Computer Security – ESORICS 2019* (2019). DOI: 10.1007/978-3-030-29959-0_28

Provided by University of Luxembourg

Citation: Researchers uncover privacy flaw in e-passports (2019, September 26) retrieved 5 May 2024 from https://techxplore.com/news/2019-09-uncover-privacy-flaw-e-passports.html