WIRED

US Border Patrol Hasn’t Validated E-Passport Data For Years

Lily Hay Newman

February 22, 2018

PASSPORTS, LIKE ANY physical ID, can be altered and forged. That's partly why for the last 11 years the United States has put RFID chips in the back panel of its passports, creating so-called e-Passports. The chip stores your passport information—like name, date of birth, passport number, your photo, and even a biometric identifier—for quick, machine-readable border checks. And while e-Passports also store a cryptographic signature to prevent tampering or forgeries, it turns out that despite having over a decade to do so, US Customs and Border Protection hasn't deployed the software needed to actually verify it.

This means that since as far back as 2006, a skilled hacker could alter the data on an e-Passport chip—like the name, photo, or expiration date—without fear that signature verification would alert a border agent to the changes. That could theoretically be enough to slip into countries that allow all-electronic border checks, or even to get past a border patrol agent into the US.

"The idea of these things is that they’re supposed to provide some additional electronic security over a standard passport, which can be forged using traditional techniques," says Matthew Green, a cryptographer at Johns Hopkins University. "The digital signature would provide that guarantee. But if it’s not checked it doesn’t."

A letter to CBP on Thursday from senators Ron Wyden of Oregon and Claire McCaskill of Missouri highlights this crucial shortcoming. More than 100 countries now offer passports that come with a digital chip, and fewer than half of those include the capability to verify the integrity of datausing a digital signature. But Wyden and McCaskill stress that while the US demands that countries in the Visa Waiver program put a chip in their passports, it has failed to fully realize its own e-Passport program.

"CBP does not have the software necessary to authenticate the information stored on the e-Passport chips," the two Senators wrote. "Specifically, CBP cannot verify the digital signatures stored on the e-Passport, which means that CBP is unable to determine if the data stored on the smart chips has been tampered with or forged."

The situation appears particularly shameful given that the US led the promotion of e-Passports around the world. "I had assumed that they would verify this," says Martijn Grooten, a security researcher for the information and testing platform Virus Bulletin. "It may cause some grumbles among countries in the Visa Waiver program: The US has demanded they offer e-Passports, and then only implemented the system partially themselves. It is a bit embarrassing."

Even worse, DHS and CBP have known about the problem for at least eight years; the Government Accountability Office issued a report in 2010detailing the need to implement signature verification for e-Passports. "DHS does not have the capability to fully verify the digital signatures because it ... has not implemented the system functionality necessary to perform the verification." GAO concluded at the time. "The additional security against forgery and counterfeiting that could be provided by the inclusion of computer chips on e-passports issued by the United States and foreign countries ... is not fully realized."

Nearly a decade later, the DHS Inspector General's list of ongoing projects requiring oversight still doesn't include rolling out the software for signature verification. US Customs and Border Protection did not return WIRED's requests for comment.

The holdup doesn't surprise longtime border security observers. "If you look at DHS’s track record on taking proposals from the RDT&E stage through validation and deployment, it’s a horrible track record," says Patrick Eddington, a homeland security and civil liberties policy analyst at the Cato Institute. "DHS and its components spend a huge amount of their time and money on big-ticket projects that generally have a much higher level of congressional interest than this particular e-Passport issue."

Researchers like Virus Bulletin's Grooten note that even without signature validation ensuring data integrity, it would still take technical skill to manipulate the information on an e-Passport's RFID chip. And actually using a digitally altered document at a border would also often require physical document manipulation and social engineering. But RFID hacking is a developed field, and researchers have even looked specifically at e-Passport manipulation and the flaws in its implementation. Researchers have especially had success cloning real e-Passort chips and then working off of the clones to build a fake accompanying document.

"It’s reasonable to guess that most passport officers go by what’s on their screen, because it’s electronic and supposedly trustworthy," says Johns Hopkins' Green. "So you could do anything from forging the expiration date of a passport to completely changing all the data, including picture, that the passport officer looks at. If they don’t double check the paper version they wouldn’t notice."

Without the ability to validate an e-Passport's signature, CBP is leaving an exposure that analysts say would cost somewhere in the low millions of dollars to solve. Of all the low-hanging fruit in government security shortcomings, this may be the lowest.