FAQ on University of Washington / RSA Labs research on Passport Cards and EDLs

v1, 2009

Karl Koscher, Ari Juels, Tadayoshi Kohno, and Vjekoslav Brajkovic
University of Washington and RSA Laboratories

Q: What is a Passport Card? How does it differ from passport?
A: The Passport Card is a low-cost alternative to the traditional passport (a "passport book") that is valid only for land and sea travel between the United States and Canada, Mexico, the Caribbean, or Bermuda---not for air travel. It is designed to meet the requirements of the Western Hemisphere Travel Initiative, a regulation that phased out the validity of drivers' licenses for such border crossings. A Passport Card has the same physical format as a credit card. It includes a wireless microchip called an RFID (Radio-Frequency IDentification) tag. The Department of Homeland Security (DHS) oversees the border-protection agency (Customs and Border Control) that makes use of the Passport Card, and has largely guided its design and implementation, while the U.S. State Department is responsible for issuing the card.

Q: What is an Enhanced Drivers' license (EDL)?
A: An EDL is a state-issued identity document that has the features of a conventional drivers' license, but additionally carries an RFID tag like that in a Passport Card. As with the Passport Card, an EDL is valid for land and sea entry into the United States. To date, Washington and New York State are the only two states that have issued EDLs. Michigan will follow soon, and DHS has signaled interest or plans on the part of Arizona, California, Texas, Vermont, as well as provinces in Canada.

Q: What does your research show about Passport Cards and EDLs?
A: The RFID devices in these identity documents are known as EPC (Electronic Product Code) tags. They are essentially wireless barcodes. That such tags have limited security features and are subject to clandestine scanning and emulation in a clone device is already widely known in the technical community.

Our research confirms the vulnerability of Passport Cards and EDLs to copying attacks of their electronic RFID components. We have shown, in fact, that an anti-counterfeiting measure that the U.S. Department of Homeland Security appears to have contemplated is not present in its initial designs is not present in the Passport Card. Without this countermeasure, it is a technically straightforward matter to copy the data from a Passport Card's RFID tag into another, off-the-shelf tag. An attacker does not have to resort to building an emulating device in order to create a radio-similar clone. (While we think it unlikely, it is possible that DHS has deployed other anti-cloning countermeasures in the field.) Our research additionally shows that the RFID tags in Passport Cards are subject to scanning at a long range---exceeding 150 feet under certain circumstances. The protective sleeve provided with the Passport Card effectively prevents such scanning.

We have also found that EDLs have weaker security properties than Passport Cards. They are subject to clandestine scanning at short range even through certain protective sleeves. Additionally, our research suggests that they are subject to clandestine, malicious destruction via radio from an off-the-shelf RFID reader.

The EPC tags in Passport Cards and EDL do not contain personally identifying information; they store what amounts to a database record pointer. Thus, concerns about read ranges revolve more around counterfeiting than privacy, though privacy is still an issue since repetitive reads of the same card can reveal travel patterns.

Our research demonstrates the systemic problems that the vulnerabilities in Passport Cards and EDLs have the potential to create, including:

1. Heightened opportunity for impersonation of travelers at the border;
2. Erosion of best practices, i.e., an insinuation of security vulnerabilities into new systems that consume identity documents;
3. Denial-of-service attacks in which malicious entities cause EDLs to self-destruct in order to create a nuisance or to undermine traveler confidence by causing a publicly visible disruption of passenger movement; and
4. Tracking of individuals through repetitive reads.

Q: Doesn't border control involve multiple layers of security?
A: While DHS does not publish the specifics of the border-crossing protocol, it is to be expected that border-control agents will not rely exclusively on RFID data. They will very likely interview passengers and perform physical inspection of their identity documents in some or all cases.

The RFID tag in Passport Cards and EDLs, however, is designed to play a pivotal role in the border-crossing process. It is scanned prior to agent-passenger interaction, and automatically guides an initial watchlist lookup. Research in psychology shows that first impressions and automated guidance have a strong influence on human decision making. Consequently, cloned EPC tags, by causing false negatives in watchlist flagging process, could have a non-negligible impact on agents' behavior and the security of our national borders.

Q: What's the difference between the RFID chips in Passport Cards / EDLs and those in passport books?
A: Passport books issued by the United States have embedded RFID tags. Those tags provide cryptographic protections against eavesdropping, which is of especial importance because they store personal information. Passport books also have metallic covers which, when firmly closed, prevent scanning of their RFID tags. The data contained in passport RFID tags is digitally signed, preventing counterfeiting (although not copying of tag contents). While not as strong as possible, these protections are probably adequate for most travelers and for ordinary security needs. (A UC Berkeley / RSA Labs paper discusses RFID security in passport books.) The RFID tags in passport books also have a considerable shorter read range than those in Passport Cards and EDLs.

Passport Cards and EDLs carry RFID devices called EPC tags that do not have cryptographic protections. EPC tags do have passwords which, when properly configured, protect against modification and destruction of their data contents. But they have no explicit anti-cloning features. Unless specially configured, they can be easily copied into other EPC tags. They are also vulnerable to cloning into emulator devices.

Q: Does your work mean that RFID is not secure?
A: The term "RFID" doesn't denote a particular product or technology. It's a catch-all term for many types of wireless identification device. Some RFID devices have stronger security features than others. As with any other technology, the challenge of system designers is to select and configure RFID devices to meet the security requirements of their deployment environments. Some (relatively expensive) RFID tags incorporate strong security features, including industry-standard cryptographic algorithms.

Q: Does your work mean that Passport Cards and EDLs not secure?
A: Passport Cards and EDLs are important instruments for the protection of our nation's borders. That said, their design aims rightly or wrong to meet tight operational constraints in the interest of affordability and passenger convenience. Our work suggests that as deployed, Passport Cards and Washington State EDLs possess security and privacy deficiencies that have the potential to compromise border security or render it more fragile than necessary and desirable. Our paper recommends some cost-effective, though partial remedies. (We have not examined the New York State EDL, but it is likely that much of our analysis applies to that identity document as well.)

We further stress that our research focuses primarily on the technical aspects of these cards. To understand whether they are secure for a real deployment, however, requires a much broader study involving border crossing officials and others.

Our study does speculate on the potential impact of our discoveries under some potential scenarios at border crossings. We stress, however, that part of these discussions are speculative. Nevertheless, we feel that the issues we raise are real and significant and look forward to working with DHS and others to determine the appropriate balances between security, privacy, and all the other related goals.

We also stress that even if the U.S. border crossings scenarios implement rigorous procedures to protect against cloning and other attacks, our results suggest that other entities considering similar deployments should be similarly wary of the issues we raise. These other entities could be other countries seeking to deploy similar technologies at their borders, or other entities within the U.S. wishing to deploy similar technologies for other purposes.

Q: What risks do the Passport Card and WA EDL pose?
A: The major risk, in our view, is that of clandestine device cloning. An attacker can in principle harvest the data from a Passport Card or EDL and create an identity document that transmits identical information (even if it does not appear identical upon inspection). If border control agents do not exercise sufficient vigilance in the passenger screening process, e.g., physical inspection of all cards, the result could be a heightened risk of passenger impersonation.

As with any RFID device, there is also the risk of clandestine tracking. The RFID tags in these documents emit unique serial numbers. While these numbers are not personally identifying in and of themselves, they are a “license plate” of sorts. For example, law enforcement officials could, in principle, scan the tags of participants in a political rally and store the associated identifiers in a database for later identification of individuals. That said, any wireless device today can be used to track its bearer. And while most RFID tags have shorter read ranges than the ones in Passport Cards and EDLs, mobile phones, on the other hand, have very long transmitting ranges. While we believe that counterfeiting is a greater concern than privacy for Passport Cards and EDLs, we still believe that privacy is a concern, particularly because there are many scenarios in which a person might have a Passport Card or EDL on them but no other trackable electronic devices.

Q: Shouldn’t the Passport Card and EDLs use RFID tags with strong cryptography?
A: Strong cryptography, that is, an industry-standard authentication algorithm, would certainly minimize the risk of cloning attacks against the RFID tags in these identity documents. It would, however, result in diminished read ranges and increased cost. An appropriate balance of security and convenience is a difficult one to achieve in any system. We believe, however, that the security of the Passport Card and EDLs can be improved without expensive changes to the system, and recommend some such changes in our research paper.

Q: What I can I do to protect myself?
A: The Passport Card and WA EDL come with protective sleeves. When in good condition, these sleeves provide robust protection against clandestine scanning of the Passport Card; they provide less protection for the WA EDL, but still have some protective value. At this stage, possession of either identity document is optional. Concerned travelers can use passport books instead for international travel.

Our belief is that the risks to ordinary individual travelers posed by the vulnerabilities we have uncovered are low. Our concern lies rather with potential systemic weaknesses in the border-crossing system.

Q: Did you inform DHS and Washington State of your findings?
A: We informed both DHS and Washington State officials of our findings in advance of their public release. We wished to offer them a timely opportunity to evaluate our research results and consider steps for strengthening the border-crossing system.

In our productive discussions with these organizations, they have indicated an ongoing effort to improve the security of the identity documents treated in our work.

Q: Why are you publishing these vulnerabilities? Will your paper have a negative impact on national security?
A: As experts in data security have believed for many years, public scrutiny makes systems stronger, not weaker. (In cryptography, this idea finds expression in a classical idea known as Kerckhoff's Principle.) The lessons and accountability brought by communal discussion are hard to obtain through restricted, closed-door assessments. Indeed, the Department of State solicited public comments on the Passport Card prior to its release, and many contributors---including four Members of Congress---expressed concerns about its security.

It is our hope that the findings in our paper will lead to stronger border security in the United States and provide guidance to other countries or organizations that look to use similar technology.

The University of Washington and RSA Labs, of course, *did not create* a vulnerability in the systems under study. We have both *identified* potential flaws and *offered recommendations*for strengthening the RFID-components of the border-crossing identification process.

Q: What are the most important lessons to be drawn from your work?
A: While our research leads to specific recommendations for strengthening the security of border-crossing systems using the Passport Card and EDLs, we believe that a more important lesson is the value of three larger essential principles of RFID security. These are guiding principles enunciated by RFID-CUSP (the RFID ConsortiUm on Security and Privacy), of which RSA Labs is a member:

- *Planning ahead*: Good security is built in, not bolted on. The Internet has taught a key lesson: It is less costly to anticipate threats and to secure systems from the start than to patch after the fact.
- *Open design*: Public scrutiny usually breeds stronger systems than private finger-crossing. Openness has long been a cardinal rule of cryptography and a pillar of secure system design. Similarly, responsible disclosure of vulnerabilities holds the technology industry to high standards and brings vital education to the community.
- *Thinking holistically*: Well conceived goals beget well conceived solutions. Thorough understanding of the uses and abuses of a system is the first step toward economical and effective security.

Q: How can I learn more about RFID security?
A: RFID CUSP (RFID ConsortiUm on Security and Privacy) is an organization devoted to academic research on RFID security and privacy. Its members include Johns Hopkins University, the University of Massachusetts at Amherst, and RSA Labs. A number of its published papers on RFID security, including some on previous security flaws discovered in RFID devices, are available at www.rfid-cusp.org. RSA Labs has published some basic primer materials, accessible at www.rfid-security.com.