RFID Passport Implementation Vulnerabilities: Technical Analysis

Kevin Mahaffey
Flexilis, kevin.mahaffey@flexilis.com

The impending implementation of RFID transponders in United States passports is nearing and currently scheduled to begin deployment in October 2006. Flexilis has found a significant problem in the State Department's proposed solution. This issue, if not immediately addressed, could put American passport holders at increased risk while traveling abroad for the 10 year lifetime of passport deployment.

In the past, the State Department has appropriately responded to demonstrable security vulnerabilities in electronic passports and will hopefully take the necessary course of action in this situation as well. In their 2005 request for comment, the State Department received over two thousand responses, the overwhelming majority of which (98.5%) were negative, mostly due to security concerns [1]. Realizing the absolute necessity of security in RFID-equipped passport documents, the State Department amended the e-passport proposal, adding additional security measures. First, Basic Access Control, an ICAO standard, was added to require authentication before a tag could be read and to encrypt data sent over the air. BAC requires that a passport reader initially make an optical scan of the machine readable zone on the inside-front cover of a passport and use that information to generate the required encryption keys. Additionally, a metal shield will be included in the front cover that will "mitigate the threat of skimming from distances beyond the ten centimeters… as long as the passport book is closed or nearly closed." [1]

Ideally, the shield is supposed to be a fail-safe, preventing any communications with the RFID transponder while the passport is not significantly open. Thus, it would be impossible to access an electronic passport without the owner's express consent manifested in the form of an open booklet. In reality, the proposed shield design permits tag communications when a passport booklet is open even a fraction of an inch as could be the case when it is carried in a pocket, purse, or briefcase.

Physically, when the passport is completely closed, the front-cover shield effectively nullifies the reader's alternating magnetic field by the generation of internal eddy currents. Because the tag is immediately adjacent to the shield when the passport is completely closed, the reader's activation field is significantly attenuated and does not affect the tag. When the passport is slightly open, the shield can no longer nullify the field seen from the tag's frame of reference; however, the proximity of a metal surface to the tag's inductor changes the tuning characteristics (resonance frequency and Q factor)

of the antenna. Instead of disabling reader communications when the booklet is slightly open, the front cover shield simply requires a stronger reader activation field to power the tag. With a medium-power reader, a RFID passport with the current security measures in place can be read when it is open just a fraction of an inch as could be the case when it is carried in a pocket, purse, or briefcase. High power readers will allow reading with even smaller passport opening dimensions, making the current shield implementation even less effective.

With regard to the real world risk associated with shield failure, there are two vulnerability-cases.

Assuming that BAC is secure, the risk of explicit information disclosure (identity theft) is minimal due to the authentication required to access any personal information; however, what security expert Jon Callas has described as a one-bit attack remains. For an attacker to authoritatively know that someone is carrying a passport (and where he or she is carrying it) is a large security threat that may subject Americans to increased risk abroad. Additionally, various characteristics (unique singulation identifiers, power analysis, etc.) can be utilized to fingerprint the characteristics unique to each country's RFID deployment and allow attackers to ascertain the exact country a given passport belongs to. Taken to a logical extreme, this could enable what has been described as a RFID-equipped mine which only detonates in the presence of U.S. citizens.

Although the cryptographic strength of BAC has been called into question, it currently provides adequate security for U.S. passports. According to one study, the current system contains keys with ~52 bits of entropy [2] which leads to a (currently) technically impractical attack. BAC, as was initially implemented in Dutch passports, has already been broken [3] due to it containing only ~35 bits of entropy. Because passports will be deployed for ten years, it is highly possible that BAC will be broken and allow attackers to access all of the personal information available on a passport. It is also important to note that the current standard specifies a large amount of storage available on the passport transponder (64 KB instead of the ICAO minimum of 32 KB) for the possibility of fingerprint or iris data in the future [1], thus making a full data compromise very undesirable.

Weak passport security directly relates to possible personal data and identity theft as well as terrorist and criminal attacks against U.S. citizens. In order to maximize the benefits of electronic passports (more authoritative identification documents, etc.) and minimize their potential risks, both increased BAC key strength and a better shielding solution need to be implemented. A modified BAC key is trivial and only relies on changing the content of the passport's MRZ or the passport numbering system. A better shield is more technically involved from a design standpoint, but would add little

to the production cost of a passport booklet when produced in volume and would add significant security enhancement.

An example of an improved shielding system for U.S. passports would be to include a conductive shield on both covers so that all reader-generated alternating magnetic fields are attenuated in the region between the two shields, namely, the inside of the passport booklet where the RFID tag is located. Such a system makes it nearly impossible to read the tag unless the booklet is open significantly more than would be probable in a pocket or purse. In order to make the tag readable only from one direction, a small tag isolation layer comprised of a material with high magnetic permeability and very high resistivity (low conductivity) such as ferrite is deposited between the tag and the shield. Thus, the system will allow full readability when the passport is significantly open and no readability when closed. To optimize this system for greatest read range when the passport is open, the tag's tuning capacitance would have to be adjusted to center the resonance frequency at 13.56 MHz. Typically, the tuning capacitor of a passive transponder is external to the IC chip and in the form of two metal layers deposited on either side of the substrate forming a near-ideal parallel plate capacitor that can be adjusted by changing the area of the parallel metal deposits on each side of the tag substrate. Alternatively, it is possible to use a dielectric (high resistivity, low magnetic permeability) spacing layer between the tag and shield; however, the dimension of such a system would likely be too thick to implement in a passport cover.

Overall, the e-passport proposal is adequate in terms of data security and will not result in identity theft as long as BAC remains unbroken; however, it is clearly lacking in physical security. Despite proposed security features, information disclosed by the RFID tag without BAC authentication is available to any attacker with the proper equipment and is sufficient to put American passport holders at greater risk of terrorist and criminal attack while traveling abroad. If the shielding system is addressed immediately, many risks associated with RFID passports will be minimized in a cost and time effective manner, offering greater security to Americans abroad for the foreseeable future.

[1] Federal Register FR Doc 05-21284, October 2005.
http://edocket.access.gpo.gov/2005/05-21284.htm
[2] A. Juels, D. Molnar, D. Wagner. Security and Privacy Issues in E-passports, 2005. IACR Cryptology ePrint Archive, http://eprint.iacr.org/2005/095
[3] Riscure, Privacy Issues with new digital passport, 2005.
http://www.riscure.com/news/passport.html