Enhancing Privacy for RFID Passports

Henning Schulzrinne
Columbia University
hgs@cs.columbia.edu

April 21, 2005

Abstract

This brief note describes how the privacy of passports containing radio frequency identification devices (RFID) can be enhanced without interfering with its functionality.

1 Introduction

The United States Department of States has proposed to issue enhanced passports that use radio-frequency identification (RFID) technology to American citizens, according to 70 Fed.Reg. 8305 (Feb. 18, 2005).

According to the proposed regulation, "the passport's electronic chip would duplicate the data that appears on the visible data page of the passport: the bearer's name, date of birth and place of birth, the passport number, the dates of issuance and expiration, the issuing authority, the document type, the passport application reference number, and the photo in digitized format. It would also contain a unique chip identification number."

Thus, the RFID chip would not contain any additional information and may well be harder to forge than paper passports.

However, privacy concerns have been raised since it appears possible for third parties to read such RFID passports from a distance of several feet, with modest technical effort, using commercial off-the-shelf equipment. This would allow individuals or organizations to "scan" individuals carrying such passports in their pockets or luggage, without the passport holder's awareness or consent. Apparently, there is no cryptographic protection of the content.

Criminals could well obtain this information and use it, for example, to forge passports or to determine who has likely left their home for an extended period of time.

2 Proposed Solution

While contactless reading of passports can be advantageous compared to traditional contact-based smart cards, e.g., avoid issues of contact contamination, the use of the RFID is only necessary when an authorized official needs to inspect the passport and associate the passport with its bearer.

Thus, a mechanism needs to be found that reliable makes the passport available for reading, but avoids unintentional disclosure of the RFID content. There have been (probably at best semi-serious) proposals to provide aluminum sheaves for the passport, as those would block the RF signals. It appears unlikely that passport bearers would remember to keep their passports in such wrappers and it would likely delay processing as customs officials remove documents from such enclosures.

Below, we propose several possible technical solutions and evaluate their applicability:

Light sensor: A light-sensitive element embedded in the passport center page only activates the RFID circuitry when sufficient light falls onto the passport. If the passport is closed, the RFID circuitry is disabled. A simple photo-sensitive resistor can serve this purpose and does not require any active circuitry. This approach is similar to one used by electronic "singing" greeting cards that play their tune when the recipient opens the card. Ambient light is sufficient to activate the circuitry, so the customs official would only have to open the passport in order to obtain the data. The additional cost of such circuitry appears extremely modest, as they can be embedded in greeting cards.

Mechanical pull-tab: Instead of light sensor, a mechanical pull-tab could activate the RFID antenna circuitry. Again, there appear to be greeting cards and children's books that use these techniques to activate electronic circuitry.

Cryptographic: The data in the RFID could be protected with the public key of the appropriate customs authorities. However, this would mean that all such authorities worldwide would have to share a private key and would risk catastrophic failure if that private key were to be accidentally disclosed.

In summary, there appear to be simple, low-cost privacy protection mechanisms that are easily verifiable in their effectiveness by third parties and do not interfere with legitimate needs of customs and immigration officials.