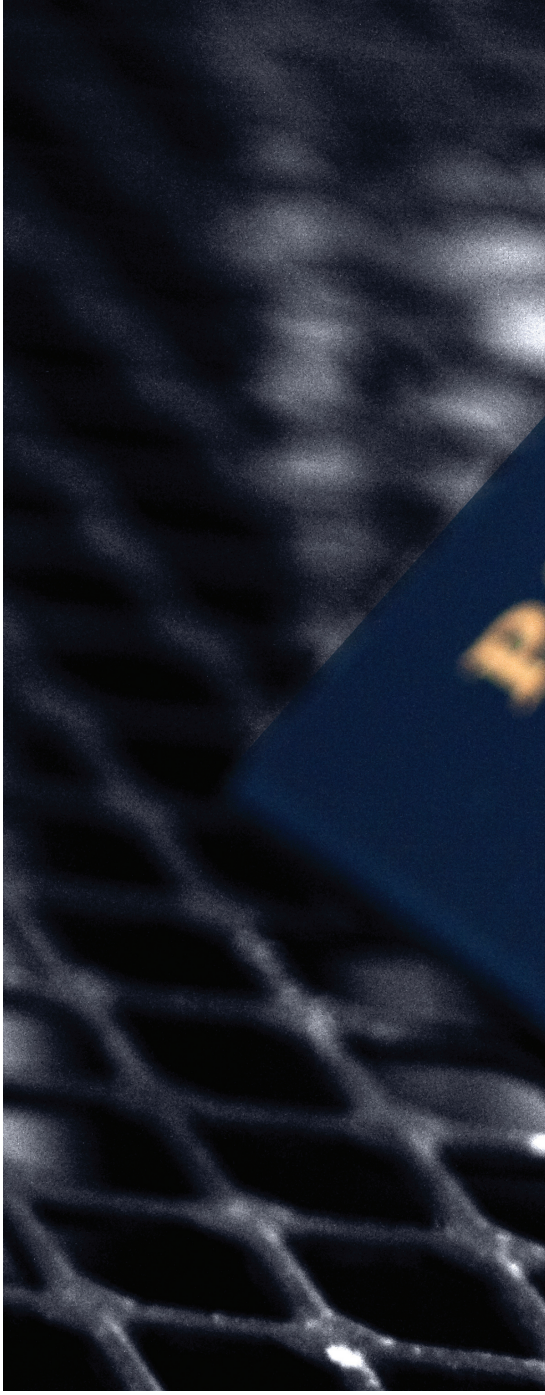
DOI:10.1145/1610252.1610268

Article development led by acmqueue
queue.acm.org

Do RFID passports make us vulnerable to identity theft?

BY ALAN RAMOS, WEINA SCOTT, WILLIAM SCOTT, DOUG LLOYD, KATHERINE O'LEARY, AND JIM WALDO

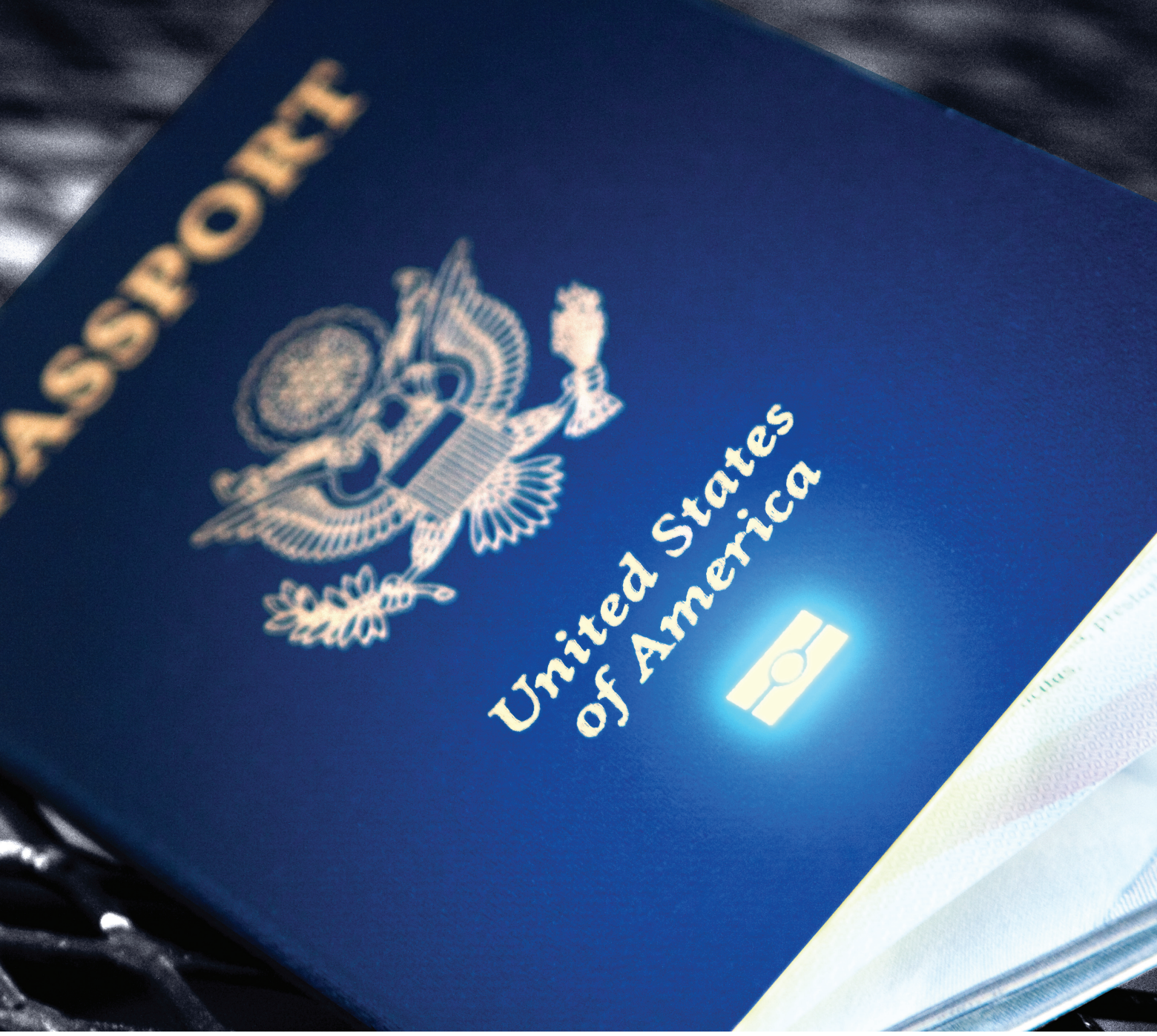
A Threat Analysis of RFID Passports



IT'S A BEAUTIFUL day when your plane touches down at the airport. After a long vacation, you feel rejuvenated, refreshed, and relaxed. When you get home, everything is how you left it—the tables, the chairs, even the now-moldy sandwich you forgot on the counter. Everything, that is, but a pile of envelopes on the floor that jammed the door as you tried to swing it open.

You notice a blinking light on your answering machine and realize you've missed dozens of messages. As you click on the machine and pick up the envelopes, you find that most of the messages and letters are from debt collectors. Most of the envelopes are stamped "urgent," and as you sift through the pile you can hear the messages from angry creditors demanding that you call them immediately. Reading the bank statements, you suddenly realize that someone has been charging large amounts of money to an account in your name from a credit card company you've never heard of. You've lost thousands of dollars, and suddenly you aren't feeling quite so relaxed anymore.

How could someone have been stealing money from you like this while you were away on vacation? The thievery actually began months before you even left home. Several months ago, as you were casually walking through the airport en route to a business meeting in Europe, someone was lingering close behind. As you approached a security agent to have your passport



PHOTOGRAPH BY BRENT HARDINGE

checked, this individual used a small antenna connected to a computer in his backpack to *eavesdrop* on the radio communication between the security agent's reader, which has the capacity to decrypt the highly sensitive and secured data on the passport, and the RFID-enabled passport itself.

If the attacker had tried to *skim* the information off your passport by imitating a legitimate reader, the chip would never have provided the personal data within, as the correct access key would not have been given. Since the attacker was merely intercepting the communication with an antenna, however, he was able to collect all of the data, albeit in an encoded form. Private information, including not only basic information about your identity but even a digitized photograph, had been stolen from you at a moment when you thought your passport was safely in the hands of a government official. You moved on without any clue as to how deeply your privacy had been violated in an attack that you had no idea was occurring.

At that point, all the perpetrator needed to do was use the data to create a new passport, use that passport to get a U.S. Social Security number (http://www.ssa.gov/pubs/10002.html), and then create credit card accounts in your name, with your identity, and run amok with your finances.

An RFID-passport attack of this nature is more plausible than other methods, such as skimming the RFID information. Although simple to do, skimming will not yield the information needed to enable identity theft because of preventive measures integrated into the system. The first of these measures is encryption. According to the U.S. Department of State: "When a reader attempts to scan the passport, it engages in a challenge-response protocol that proves knowledge of the pair of keys and derives a session key. If authentication is successful, the passport releases its data contents; otherwise, the reader is deemed unauthorized and the passport refuses read access."[6]

Additionally, newer passport covers are being lined with materials that block RFID signals from being transmitted when the passport is closed, exposing the document to attack only when it is opened and displayed for a security agent. Relatively inexpensive signal-blocking sleeves (http://www.rfid-shield.com/products.php) are also available for RFID passports.

What Information is Compromised?

Six pieces of information can be stolen from the RFID chip on a U.S. passport: your name, nationality, gender, date of birth, place of birth, and a digitized photograph.[1] Numerous problems of identity theft could arise from someone taking that information, but this article focuses on the financial risk.

Banks in the U.S. require that applicants for credit cards submit their Social Security numbers to be used for background credit checks. Although the passport RFID tag does not carry your Social Security number, a perpetrator can use the information it does contain to obtain your number.

The Social Security Administration's Web site (http://www.ssa.gov/pubs/10002.html) requires one of three proofs of identity for a U.S. citizen to be issued a new Social Security card: a driver's license, state-issued non-driver identity card, or passport. With the data stolen from your passport's RFID chip, someone could create a copy of the passport, then use this counterfeit one to access a real copy of your Social Security card. With this card, the perpetrator is free to apply for a real copy of your credit card, not to mention opening new accounts in your name. This puts you at a serious financial risk, all because someone was able to eavesdrop on your passport's RFID communication.

Technology Requirements

To eavesdrop on your passport information, a perpetrator needs hardware to capture the signal as it is being scanned by a legitimate RFID reader, such as those used by government officials at airports. He or she would then need the time and technical capacity to decrypt the signal into a usable form. Finally, to reap any real benefits from the stolen information, the attacker must have all the materials necessary to reproduce a passport. We can view this as a series of hurdles that the perpetrator must overcome, starting with data capture, moving onto data recovery, and finally data reproduction.

Six pieces of information can be stolen from the RFID chip on a U.S. passport: your name, nationality, gender, date of birth, place of birth, and a digitized photograph.

Let us first focus on capturing the information from your passport, since it is at that point in the event chain that the vulnerabilities of the RFID technology are exploited. For successful data retrieval the perpetrator's antenna must catch two different interactions: the forward channel, which is the signal being sent from the RFID reader to the RFID token; and the backward channel, which is the data being sent back from the RFID token to the RFID reader. Lab demonstrations[3] have shown that a successful eavesdrop (a capture of both channels) on an RFID tag can occur at a distance of one meter with the use of an H-field antenna, a radio frequency receiver, an oscilloscope to monitor the signals, and a computer to store, analyze, and manipulate the data.

In the lab this was done as a proof of concept, but in the real world a perpetrator could use smaller, more discrete hardware. In our airport scenario, the perpetrator would need only an antenna and an amplifier to boost the signal capture, a radio-frequency mixer and filter, and a computer to store the data. The amplifier itself would not even need to be that powerful, since it would need to boost the signal over only a short distance of three to five meters. The antenna, mixer, and filter can be homemade with cheap materials or purchased as a set online. Some Web sites (for example, http://www.openpcd.org/openpicc.0.html) contain schematics, lists of materials, and steps on how to build your own RFID reader the size of a matchbox. These RFID "sniffers" can then be plugged into a laptop via a USB port.

Once the perpetrator has successfully eavesdropped on the communication between the RFID token and the RFID reader, the next step is data recovery. This requires two separate steps. The first is recovering the actual signal between the RFID chip in the passport and the RFID reader. This is a signal-processing problem, essentially separating the actual signal from the noise of the background. Proof-of-concept experiments[3] have shown that data recovery is a brute-force problem that can be solved with current hardware. A

perpetrator would need only to record the data passed between the RFID and receiver on location, and then could perform the time-consuming signal-processing operations at home. A large part of data recovery is extracting the data from the electrical noise of the environment, which is simplified by taking a noise profile of the environment. The same Web sites that provide schematics for readers also provide code for decoding the data, although the effectiveness of their programs on new passports has yet to be tested.

Once the signal has been recovered, it must be interpreted as data. The difficulty of this step depends entirely on whether and how well the data is encrypted. The encryption key is generated from information on the passport—specifically, the name, date of birth, and passport number. There are reports that this key can be easily cracked (for example, http://www.mobilemag.com/2006/02/03/global-rfid-passport-encryption-standard-cracked-in-2-hours/) because the algorithm used to produce the key is predictable. An analysis published by the International Association of Cryptologic Research indicates that the entropy of the resulting key is on the order of 52 bits, which, while something of a challenge, is not impossible to crack.[4] We assume here that decryption is practical; if it is not, then the possibility of these attacks is minimized.

After recovering the data, the perpetrator would have everything necessary to make a new passport with the captured information. The steps required for this are beyond the scope of this article, but since counterfeiting of passports has been demonstrated and documented, it is enough to say that this is feasible.

Costs to the Perpetrator

What we have shown so far is that with the right equipment and skill, a perpetrator can intercept the signal between a passport and RFID reader, then forge the passport to use for identity theft. The more important question, however, is whether the cost of doing this can be justified by the return.

This question is predicated on the assumption that the encryption of the information held in the passport's RFID tag can be broken. While there is some evidence this has been true in the past, stronger encryption could increase the cost of the attack considerably, to the point of making it either economically unattractive or technically impossible.

In our airport scenario, a perpetrator would have to cover several costs before reaching the ultimate goal of financial gain. To begin with, there are the hardware costs. The combined cost of the antenna, amplifier, radio mixer, filter, USB connection, and laptop would be on the order of $1,000. These are all fixed costs, and the perpetrator would presumably amortize these by using the hardware to execute numerous attacks over a period of time.

There is also cost associated with access to the passport reader. It is reasonable to assume that the perpetrator would have to purchase an airline ticket to enter the area where passports are scanned.

The cost of being caught must be factored in. Compared with other technologically intensive (for example, online) fraudulent attacks, theft of passport RFID data might involve greater risk because of the physical proximity required to eavesdrop on the RFID communication. The risk-adjusted cost of being caught is quite significant when you consider the prevalence of security officers within airports and the severity of the crime.

Presuming that the attacker manages to escape with the raw data from an eavesdropping operation, it still

PHOTOGRAPH BY ALEX GRIMM/GETTY IMAGES

EasyPass, a new automated border control system at Frankfurt International Airport, scans passenger biometric data and compares it to data from the person's e-passport.

has to be interpreted at home. The software costs are negligible (open source code for this specific function is available on the Internet) as are the costs of the processing time. In one example, it took less than an hour to recover the passport signal, and this process can be automated.[3] Although we have not verified this (since verification would require snooping a passport in a noisy environment such as an airport), the approach presented seemed plausible.

Jeroen van Beek of the University of Amsterdam managed to forge a passport RFID chip for $120.[5] This cost is not always necessary because a U.S. passport remains valid even if it is not fitted with an RFID chip or if the chip has failed. (Since all passports issued after 2007 have an embedded RFID chip and are valid for a maximum of 10 years, the ability to use a passport without such a chip will end after 2017.) Rather, the most significant cost is in obtaining or producing a realistic-looking passport in which to print the information. The cost of a blank passport book is difficult to determine, but there are some indications that it is not an insubstantial part of the cost of this form of identity theft. In 2008, for example, 3,000 blank U.K. passports were stolen, and officials valued each one at approximately $3,000.

Estimating the revenues that could be generated also requires some inference. In the U.S., the mean fraud amount per victim for identity theft-related crimes in 2008 was $4,849.[2] The potential revenue from the passport identity theft example, however, could conceivably be higher because of the relative ease with which a passport can be used to open new accounts and prove identity, in comparison with the most common current forms of fraud using stolen credit cards, checks, or mail. Nevertheless, comparing this figure to the $3,000 cost of a blank passport (which is just one of the many costs of creating a fake passport) reveals that the operation may not be as profitable as one might have thought.

Countermeasures

A number of countermeasures have been suggested to protect against RFID privacy risks (not specific to the passport example), including permanent tag deactivation ("killing"), temporary tag deactivation (such as using Faraday cages or sleep/wake modes), and access-control mechanisms (hash locks, pseudonyms, blocker tags). You could "kill" the RFID tag (hitting the chip with a hammer does the trick), since, according to the State Department's Web site, if the chip fails, the passport remains valid; however, most "killing" methods leave evidence of intentional damage. The other solutions would not prevent the interception of communications between tag and authorized reader, particularly at an airport.

More effective countermeasures require changes to current government policy. The government can take steps to improve the security and privacy of passports. The basic access-control system of a U.S passport encrypts communication between it and the RFID reader with a key generated from information written on the passport; the key containing the holder's information is susceptible to brute-force attacks, however, since it has low entropy.[4] One countermeasure would be to add a 128-bit secret, printed on the passport and unique to each passport, to the key derivation algorithm.

The interception of communications between RFID tag and reader is possible because no material capable of blocking RF signals surrounds the passport-control area. Thus, another countermeasure would be to install an enclosure to block RFID transmission outside of the immediate area. Increased security around the passport-control area could also minimize the possibility of intrusion on the communication between tag and reader.

The Final Analysis

Having looked at the potential attack, the costs of that attack, and the returns, we can now ask how concerned we should be about such an exploit. Should you really be worried as you walk through the airport that someone behind you might be stripping you of your passport information in a grand scheme to rob you?

The technical hurdles are surmountable, at least in proof-of-concept demonstrations. It is possible that such an attack could occur, but this possibility must be balanced against the complexity of the attack, the difficulty of obtaining the required high-priced blank passport, and the limited return the attack is likely to produce.

It seems much more likely that most perpetrators would resort to old-fashioned means of stealing your passport information, by stealing your physical passport itself. We recommend that it is more important to be careful about keeping your physical passport safely in hand than to be wary of perpetrators lurking behind you in line at the airport attempting to exploit the RFID tag in your passport. C

Related articles on queue.acm.org

Communications Surveillance: Privacy and Security at Risk
Whitfield Diffie and Susan Landau
http://queue.acm.org/detail.cfm?id=1613130

Four Billion Little Brothers? Privacy, mobile phones, and ubiquitous data collection
Katie Shilton
http://queue.acm.org/detail.cfm?id=1597790

The Magic of RFID
Roy Want
http://queue.acm.org/detail.cfm?id=1035619

References

1. Broache, A. RFID passports arrive for Americans. CNET News (Aug.14, 2006); http://news.cnet.com/RFID-passports-arrive-for-Americans/2100-1028_3-6105534.html.
2. Claburn, T. Identity thieves face pay cut. *Information Week* (Feb. 11, 2009); http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=213403976.
3. Hancke, G. Eavesdropping attacks on high-frequency RFID tokens. RFIDBlog (July 11, 2008); http://www.rfidblog.org.uk/Hancke-RFIDSec2008-Talk.pdf.
4. Juels, A., Molnar, D., Wagner, D. Security and privacy issues using e-passports. *International Association of Cryptologic Research Cryptology*, ePrint Archive; http://eprint.iacr.org/2005/095.pdf.
5. Timmer, J. Faking passport RFID chips for $120. *Ars Technica.* (Aug. 7, 2008); http://arstechnica.com/security/news/2008/08/faking-passport-rfid-chips-for-120.ars.
6. U.S. Department of State. *The U.S. Electronic Passport Frequently Asked Questions.* (Feb. 27, 2009); http://travel.state.gov/passport/eppt/eppt_2788.html#Twelve.

Alan Ramos graduated from Harvard University in June 2009 and is an independent media consultant.

Doug Lloyd graduated from Harvard University in June 2009 and is starting law school at Northeastern University, Evanston, IL.

Katherine O'Leary, **William Scott**, and **Weina Scott** are undergraduates at Harvard University, Cambridge, MA.

Jim Waldo is Professor of the Practice at Harvard University, Cambridge, MA, where he teaches distributed computing and topics in the intersection of policy and technology in the department of computer science. He is also a Distinguished Engineer with Sun Microsystems Laboratories, where he investigates next-generation large-scale distributed systems.