Preventing Attacks on Machine Readable Travel Documents (MRTDs)

Gaurav S. Kc[1] and Paul A. Karger[2]

[1] Columbia University
450 Computer Science, 1214 Amsterdam Ave., MC 0401, New York, NY 10027, USA
gskc@cs.columbia.edu
[2] IBM Research Division, Thomas J. Watson Research Center,
PO Box 704, Yorktown Heights, NY 10598, USA
karger@watson.ibm.com

Abstract. *After the terror attacks of 9/11, the U.S. Congress passed legislation that requires in the US Visa Waiver Program to begin issuing issuing machine readable passports that are tamper resistant and incorporate biometric and document authentication identifiers. The International Civil Aviation Organization (ICAO) has issued specifications for Machine Readable Travel Documents (MRTD) that are equipped with a smart card processor to perform biometric identification of the holder. Some countries, such as the United States, will issue machine readable passports that serve only as passports. Other countries, such as the United Kingdom, intend to issue more sophisticated, multi-application passports that can also serve as national identity cards. We have conducted a detailed security analysis of these specificationsm, and we illustrate possible scenarios that could cause a compromise in the security and privacy of holders of such travel documents. Finally, we suggest improved cryptographic protocols and high-assurance smart card operating systems to prevent these compromises and to support electronic visas as well as passports.*

1 Introduction

The International Civil Aviation Organization (ICAO) has been developing standards for the next generation of passports, the latest version of which was released in October 2004. The most important change in these standards is the embedding of a contactless, smart card processor chip within the passport booklet. The processor will be used to store specific biometrics of the document holder in addition to some personal information. The stored information can then be presented to border control officers at the time of travel. The new passport design is intended to serve two purposes: (a) the biometric information can be used for identity verification at border control, and (b) cryptographic technologies can be used to ascertain the integrity and originality of passports, thus preventing high quality passport forgeries that might otherwise pass a visual inspection.

While the general ideas and advantages of these passport standards are clear, there are inherent problems in the actual design decisions made in the standards.

This paper reports the result of our analysis of the ICAO specifications for the next generation of passports, and associated standards documents from standards organizations such as the International Standards Organization (ISO) and Federal Information Processing Standards (FIPS). This paper also introduces techniques and suggestions for changing the ICAO specifications to provide better security and privacy guarantees.

The paper does not address the political and civil liberties questions of biometric-based identification. That is a question for political debate [18, 38]. Rather, the purpose of this paper is to perform a security and privacy vulnerability analysis of those ICAO specifications in the context of both the simple passport application and the more complex multi-application credentials. The paper will show that, as currently written, the ICAO specifications suffer from a number of vulnerabilities that could result in a variety of privacy problems that could lead to identity theft crimes. More seriously, the paper will show vulnerabilities that will permit the exposure of the biometrics of legitimate passport holders to the very criminals that the biometric passports are supposed to protect against. Armed with those biometrics, attackers could possibly gain access to other critical sites that depend on biometric authentication. The paper will show how the ICAO specifications could be improved to avoid such problems, using techniques that can be deployed with currently available smart card technology, albeit possibly with an increased cost for each passport.

The primary breach in the security of the electronic passports arises from the invalid assumption that all communications in which a passport chip may participate are secure and legitimate. We will show how this assumption can make it possible to stalk selected passport holders, how it can facilitate identity theft crimes, and how a previous version of the ICAO specification [10, 14] could actually have facilitated passport forgery via a splicing attack. Fortunately, the latest version of the ICAO specification [15, 32] resolves this particular forgery problem, but the stalking and identity theft problems remain.

There are numerous other issues related to the use of both biometrics and smart cards with identity documents such as passports. These issues include the debates over the appropriateness of national identity cards, the reliability and lifetime of the contactless chips and antennae, whether governments should be able to track the movements of its citizens and visitors, and the reliability of biometrics in general. All of these issues are outside the scope of this report — we focus purely on the security and related technical aspects of using smart cards for electronic identity verification and document integrity verification purposes. Can the smart cards achieve their stated goals while not creating other serious problems, such as identity theft?

It is not the intent of this paper to be overly harsh on the process followed by ICAO to develop the standards. Getting wireless security protocols to be secure is a very hard task. From the track record of other major wireless security protocol developments, it is not surprising that ICAO has had problems. Among the protocols that have had similar problems are 802.11 [16], Cellular Digital Packet Data (CDPD) [17], cell phones [35], Intelligent Transport Systems (ITS) [30], and many others. These problems arise, because the designers of a wireless protocol frequently focus on the issues of getting the protocol to work and do not understand many of the subtle security and privacy implications. Such projects need to do comprehensive vulnerability analyses to ensure not only the security of the protocols themselves, but also that side effects of the protocols do not create problems for other systems.

What are the new results of this paper?

The work reported in this paper began in 2003, and some of the vulnerabilities we found have been reported since then by other authors [26]. This material is included in this paper so that the reader can fully understand the context of the problems.

However, this paper documents several vulnerabilities that have not been previously published, such as the splicing attacks in section 4, the attacks possible by hotel or bureau de change clerks who need to see passports but should not have access to the biometrics in section 5.2, fake finger attacks also in section 5.2, and weaknesses in the BSI proposal for extended access control in section 7.

The paper also proposes the use of stronger cryptographic protocols that can provably preserve the privacy of the passport holder in section 7, and shows how a high-assurance smart card operating system could not only support better security for electronic passports, but also support electronic visas in which multiple countries would be able to write to separate areas of the smart card memory in section 9.

2 Overview of Machine Readable Travel Documents

The International Civil Aviation Organization (ICAO) is a specialized agency of the United Nations that promotes civil aviation, including setting standards for passports, visas and other travel documents. ICAO formed a Technical Advisory Group (TAG) on machine readable travel documents (MRTDs) consisting of government representatives from 13 member states. Within the TAG, there is a New Technologies Working Group (NTWG) that has done the work on smart-card-based biometric passports.

In 2002 the U.S. Congress passed the Enhanced Border Security and Visa Entry Reform Act [51]. Section 303(c) of that act requires that countries that participate in the US Visa Waiver Program have a program to issue machine readable passports that are tamper resistant and incorporate biometric and document authentication identifiers that comply with standards established by ICAO. In the interest of international reciprocity, the U.S. will issue similar machine readable passports to U.S. citizens.

In 1980, ICAO introduced the use of machine-readable data printed on the data page of passports with Optical Character Recognition (OCR) text. This OCR information called the Machine-Readable Zone (MRZ) consists of the document holder's name, date of birth, sex, the document's identification numbers and validity dates.

The next stage in machine-readable data was the use of 2-D barcodes. These can be used to encode ≈ 8000 bytes of information, and are in current use on many passports, visas, and driving licenses. The applicable standards for these 2-D-barcode-based MRTDs have been published in [36].

ICAO's standards for the next generation MRTD specify [6] a contactless smart card microchip, conforming to ISO 14443 [21], to be embedded within the passport booklet. These chips will be embedded along with their antennae, which, when brought into an appropriate electromagnetic field, will generate an electric current that can power the chip.

Contactless smart cards and Radio Frequency Identification (RFID) tags are closely related technologies that are often confused. For example, the press often describes the new passports as using RFID technology, whereas the ICAO requirements in fact call for contactless smart cards. The principal distinction is that RFID tags tend to be low-cost low-end devices that can transmit a fixed message, while contactless smart cards typically have complex CPUs and cryptographic capabilities. The Smart Card Alliance has published a summary of the differences between RFID tags and contactless smart cards [40]. As chip densities increase, the distinctions between RFID tags and contactless smart cards will become less and less.

Contactless smart cards offer several advantages over contact smart cards, including no wear and tear of the physical contacts, faster data transmission rates, and not needing to change the physical appearance of a passport by adding electrical contacts. However, contactless smart cards have two potential disadvantages. Because the information is transmitted as radio-frequency signals, it may be possible for unintended recipients to intercept information. Second, if many contactless smart cards are physically close together, a reader will have difficulty sorting out which transmission comes from which card. This mutual interference problem is discussed more in section 9.

There have been multiple proposals to use the ICAO biometric passport technology for national identity cards and other purposes. The United Kingdom began with a proposal for a combined driver's license and passport [25] that has evolved into a full national identity card bill in Parliament [22]. However, the proposal has come under extensive debate [49], but it appears likely to pass as of the date when this paper is being written. Similar projects are underway in a number of countries, including Estonia [48] and Singapore. The ICAO biometric passport technology might also be used for US driver's licenses to meet the requirements of the REAL ID Act of 2005 [52], although no such requirement has been defined yet.

An important question is whether the ICAO specifications meet the intent of the US Congress in the Enhanced Border Security and Visa Entry Reform Act of 2002 [51]. The law itself does not give reasons for its requirements. Congressional intent can only be determined from the debates over the act. In this portion of the debate [53], it is clear that the Senate was most concerned about known terrorists not being detected when they entered the Unites States and that the 9/11 terrorists had overstayed their visas. While the ICAO specifications may technically meet the needs of border crossing authorities, additional concerns arise in the deployment of the proposed technology. For example, the new technology may facilitate attack on security checkpoints other than those at border crossings, as described in section 5.

3 Operation of MRTDs at a Border Post

The document holder presents his or her travel documents to the border control officer who can read the stored data from the chip after exchanging encryption keys for secure communications. The border control officer would perform a check that the passport holder actually matched the stored biometrics. The more cryptographically interesting steps in this electronic interaction can be summarized in the following: (a) Basic Messaging and Access Control, and (b) Active Authentication. Basic Messaging serves to setup an encrypted communications channel between the border control reader device and the passport chip, and the Active Authentication phase is used to verify the integrity of the travel document and provide assurance that it has neither been tampered with, nor is a forgery. Each of these steps is discussed in more detail below.

4 Passive Authentication

The ICAO specifications have both mandatory and optional features for security and authentication. The mandatory features are quite weak, and the optional features are quite limited. The only mandatory requirement is that the information stored on the contactless smart card chip be digitally signed by the issuing country and that the digital signature be checked before use. This requirement is called *passive authentication*, and it provides no protection against unauthorized disclosure of the information.

As originally conceived by ICAO [10, 14], passive authentication suffered from a serious security problem. The 2003 specifications required that the biometrics and the passport holder's name, date of birth, etc. be digitally signed separately.

With only separate signatures, counterfeiting biometric passports is easy. An attacker would get a passport with his/her own identity and biometrics. The attacker would then listen to the communications of a legitimate passport holder and get a copy of the legitimate person's digitally signed identity. The attacker could now create a new smart card with the attacker's biometrics but with the legitimate person's digitally signed identity spliced in. Each signature could be verified by border control personnel, but since the signatures were completely independent, there was no way to detect that the data had been spliced together.[3]

What was missing from the 2003 specifications [10, 14] was a requirement to cryptographically bind the identity of the passport holder together with the biometric. The problem was solved in the 2004 specifications [32, section 2.3.1] by storing hashes of all the fields in the document security object and then having the issuing authority digitally sign the entire document security object (including all the hashes). With the addition of cryptographic binding, splicing becomes impossible, because the hash in the document security object would not match the hash of the false identity. If the attacker tried to change the hash as well as the identity, then the digital signature verification would fail, and the attack would be detected.

Passive authentication provides no protection against skimming or eavesdropping attack by outsiders. A skimming attack is when someone attempts to read the passport chip simply by beaming power at the passport. At normal power ranges, contactless smart card readers must be relatively close to the card within a few inches or at most a few feet. However, that range can be extended if the reader broadcasts power at illegally high levels. A skimming attack could be done to facilitate identity theft or to trace the movements of an individual. A person traveling in a bad neighborhood could be attacked just on the basis of his or her nationality, revealed through skimming.

[3] Our work on these vulnerabilities began in 2003, and we discussed these attacks, including particularly the splicing attack, with the U.S. State Department privately at the Third Annual Smart Cards in Government Conference in March 2004.

An eavesdropping attack can occur, if the contactless smart card is actively communicating with a legitimate reader. RF emanations from both the smart card and the reader have been shown in tests to be readable at distances up to 9 meters [41, 55]. The reports of successful eavesdropping at 9 meters do not include any technical details of how the eavesdropping was accomplished. Kfir and Wool [31] report (with technical details) a successful attack at 50 meters that does not require the card to be in use in a legitimate reader.

5 Basic Access Control

The ICAO specification [32, section 2.4] suggests that some countries might be concerned about unauthorized skimming or eavesdropping and offers a basic access control mechanism as an optional countermeasure. Given that skimming and particularly eavesdropping are possible attacks, countries that choose to implement only passive authentication will leave many of their passport holders vulnerable to attack. However, this section will show that even the basic access control option is not very effective at protecting the sensitive information on the MRTD chip, such as the digitized biometrics.

Basic Access Control requires that the initial interaction between the embedded microchip in the passport and the border control reader include protocols for setting up a secure communication channel. The reader first acquires the MRZ information from the data page of the passport, generally via a connected OCR scanner. This MRZ information is used for computing the encryption and message authentication keys used for the "secure" exchange of the session keys. Using information that is available on the actual travel document is intended to limit access to only those people who have been physically shown the passport by the passport holder. Both the reader and the embedded passport chip generate, and exchange random numbers which are then used to create a shared triple-DES session key for encrypted communications.

Basic access control should be effective against simple skimming attacks. If the attacker has no knowledge of who the intended victim is, then the attacker will not know the MRZ information and will not be able to derive the cryptographic keys. However, a more sophisticated attacker who knows something about the intended victim can be more successful.

The U.S. State Department had come under significant criticism [38], because it had planned to only require passive authentication on U.S. passports. However, in April 2005, they announced [56] that U.S. passports would use Basic Access Control and attempt to provide Faraday cage shielding for passports. This was greeted positively by the press and the civil liberties community, but the limitations of Basic Access Control, discussed below, were not recognized.

5.1 Insufficient Entropy

The MRZ information used for basic authentication is the passport serial number, the holder's date of birth and the expiration date of the passport. While an attacker who is just trying to skim information off passports of random passersby would likely not know this information, someone who is trying to target a known person would certainly know at least their date of birth. Even a random attacker could guess the passport holder's age within 10 years. Since passport serial numbers are usually assigned in sequence, there is likely a high correlation between the serial number and the dates of issue and expiration. The ICAO's Public Key Infrastructure (PKI) report [32] points out that there is insufficient entropy in these numbers to protect against a serious brute-force attack, in which the attacker tries to guess the serial number and date of expiration. The report dismisses this threat, suggesting that there are easier ways to obtain the information stored on a passport.

However, the report neglects the fact that the biometric information, digitally signed by the appropriate government office is **not** easily obtained from other sources. The digital signature of the biometric particularly increases the value. In addition, the report does not consider the possibility of an attacker seated close to the intended target (perhaps on a train[4]) having a very long period of time to carry out the brute force attack of guessing all possible serial number - expiration date pairs.

The feasibility of the entropy attack has been demonstrated [54] against Dutch passports by Marc Witteman of the Dutch security company, Riscure. Witteman reports that Dutch passport numbers are assigned sequentially with an internal checksum digit. As a result, he estimates that the effective entropy of a Basic Access Control key on a Dutch passport is about 35 bits and that can be broken in under two hours on an average personal computer. By contrast, Juels, Molnar, and Wagner [26] estimate that the US passport has about 54 bits of entropy, mostly due to longer passport numbers and passport lifetimes.

5.2 Legitimate Passport Users Have Different Rights

Juels, Molnar, and Wagner [26] have discussed some of the attacks that we have seen thus far in this paper, although they did not identify the splicing attack. However, this section describes new and more serious threats than the brute force attack on Basic Access Control that have not previously been published.

The PKI report assumes that anyone who can see the printed material on the passport is allowed to read the biometrics. This is true for border control officers,

[4] Such an attack would be more difficult on an airplane, because of the restrictions on the use of radio frequency electronic equipment.

but many other staff at airports need to see the passport data page, but should not be allowed to read the biometrics. In addition in many countries, passports must also be shown to hotel clerks, and in some countries, may have to be left overnight with the hotel or with local law enforcement agencies. Furthermore, hotel clerks often photocopy the passport data page, and these photocopies will have all the information needed to pass the authentication challenges. A person may have to show their passport when changing money or cashing checks. Hotel clerks and clerks in a bureau de change should not have access to the digitally signed biometrics, but nothing in the ICAO requirements prevents this. This problem is still of limited concern if only the ICAO-required information is stored on the passport, but some countries have announced plans that the passports will become the national ID card to be used for many purposes besides international travel. If the card is your driving license, then the rental car clerks will have access to your biometrics. If it is your medical card, then clerks in pharmacies will have access. As a national ID card, more information will be protected by this inadequate authentication scheme, and the threat of identity theft becomes a very real one.

However, identity theft is not the biggest problem. If an attacker can gain access to fingerprint information stored on the card, then the attacker may be able to create a false finger [37, 47] to be used to attack unattended fingerprint reader systems. This attack could give access to critical locations to the very criminals against whom the biometric passports are supposed to protect.[5]

Fake fingers could also be a threat to the passport system itself. Malaysia [27] is using biometric passports to allow unattended border crossings for Malaysian citizens. They are assuming that if the fingerprint check is passed, then the person is authorized to enter the country. However, an attacker with a fake finger could defeat this system. The human border control officer can defeat this attack by watching for the use of fake fingers. Remote monitoring with cameras will likely be less effective, there may be many checkpoints at a busy border-crossing point, and with only a camera monitoring, it may be easier for the attacker to conceal the use of the fake finger.

---

[5] Of course, attackers can obtain fingerprints by other means, such as lifting a print off of a glass in a restaurant. However, lifting a print is difficult, because the print might be smeared. Getting the digital form of a fingerprint (either an image or minutia) gives the attacker an exact copy of what will be checked in some other biometric access control device. This makes it easier to construct a fake finger that has the correct biometric. Even this doesn't guarantee a usable fake finger, as there are liveness detectors that may be used, but anything that helps the adversary to construct the fake finger should be avoided. The current basic access control does not adequately protect the biometrics. See section 7 for a discussion of how ICAO proposes handling this.

6 Active Authentication

Once the secure communications channel has been created, the reader can verify the integrity of the data stored in the passport chip through the use of a Public Key Infrastructure (PKI). In a nutshell, the reader issues a cryptographic challenge, which is digitally signed by the passport chip. In the reader's view, this digital signature serves to affirm the authenticity of the travel document and that the chip has not been replaced.

The appendix discusses a potential issue with Active Authentication called the "Grandmaster Chess Attack".

7 Extended Access Control to Additional Biometrics

In section 5 above, we criticized basic access control as being insufficient to protect fingerprint biometrics. This criticism is technically unfair to ICAO, because the PKI technical report realizes that additional biometrics do need additional protection. The problem is that the PKI report leaves this additional protection unspecified, which means that different countries may implement different, mutually-incompatible mechanisms, and that some countries may add biometrics and not do extended access control at all.

Dennis Kügler, of the BSI in Germany, is developing such an extended access control mechanism [34] for a European Union passport specification.

Kügler's protocol consists of three major steps: 1) Basic Access Control, 2) Chip Authentication, and 3) Terminal Authentication.

After Basic Access Control, the reader is allowed access to the Document Security Object (that contains the digital signatures). Using the cryptographic key obtained through Basic Access Control, the reader carries out chip authentication and the reader and the chip derive a stronger session key from a Diffie-Hellman key pair, and use that key to protect the facial image. After the facial image has been checked, the reader carries out a two move challenge-response protocol that provides unilateral authentication of the inspection system. Only after the reader has been authenticated to the chip, does the chip reveal more sensitive biometrics, such as fingerprints.

Kügler's protocol provides much better security between the chip and the reader than does Basic Access Control. However, Kügler's protocol still has weaknesses. Because it uses Basic Access Control to derive the first cryptographic keys, those keys still have insufficient entropy. Anyone who can break those keys as shown in section 5 can gain access to the identity of the passport holder and the holder's picture, but not the more sensitive fingerprints. Note that this is sufficient information to permit unauthorized tracking of the passport holder's movements. Even if you performed terminal authentication before releasing the passport holder's identity and facial image, the Document Security Object contains enough information to track the individual's movements.

The weaknesses of Kügler's protocol are unnecessary. The Caernarvon authentication protocol [44] avoids the problems by not using Basic Access Control at all. The Caernarvon protocol preserves the passport holder's privacy by revealing nothing until the reader has been authenticated. Very briefly, the Caernarvon protocol generates a Diffie-Hellman session key first to protect all subsequent communications from external eavesdroppers. Then it requires the reader to authenticate itself to the chip, and only after the chip has determined that the reader is authorized, does the chip reveal any information at all about the passport holder.

Basic Access Control was attractive to ICAO, because it needed no public key cryptography and no public key certificate infrastructure. However, the Kügler protocol has already accepted the need for public key algorithms and certificates. There is no longer any justification for the use of weaker protocols.

The Caernarvon authentication protocol [44] was specifically designed to protect the privacy of a smart card holder and is based on the SIGMA family [33] of protocols that form the basis of the Internet Key Exchange Protocol (IKE) [20]. Not only are the SIGMA protocols a widely used standard, they have also been formally proven correct [9]. By contrast, the authors are unaware of any formal proofs of correctness of the ICAO protocols [32]. Kügler does offer a proof of his chip and terminal authentication steps, but not of Basic Access Control. IBM, the developer of the Caernarvon authentication protocol, has chosen not to assert any IP claims on the protocol, to ensure that it can be freely used in standards. As a result, the Caernarvon protocol has been adopted [3] for use by CEN, the European Committee for Standardization.

8 Other Weaknesses and Recommendations

8.1 Combining traditional attacks with biometrics

There are a host of obvious attacks against the passport-issuing systems that are quite difficult to combat. We mention some of them here, but they are not the focus of the paper. Obviously, the passport issuing system could be attacked by burglars or by people who bribe or threaten the staff to issue false passports. These attacks work against traditional paper passports as well as biometric smart-card based passports. However, if a criminal can bribe or bully an official to issue a false biometric passport, the criminal can now take advantage of human nature. Border crossing personnel are trained to detect false passports. However, human nature is such that if the computer says that biometrics are correct, the immigration official is less likely to question either the passport or the criminal.

8.2 Contactless Identification Numbers

Schneier [45] points out that even with Basic Access Control, ISO 14443A requires an identification number for the chip be transmitted unencrypted to resolve RF conflicts. This identification number needs to be assigned randomly, each time the chip is started. If the identification number remains fixed, it could be used to track the movements of the passport holder. This problem would exist, even with either Kügler's or the Caernarvon authentication protocol unless the low-level radio handling code on the chip were fixed.

8.3 Trusted Third-Parties

An alternative to mutual authentication between the reader and the passport chip would be for both to communicate with a mutually trusted third-party. In the case of a shared root certification authority, this third party would be ICAO or the UN. However, finding a third party that all countries could agree upon is likely to be very difficult. In the current proposals, ICAO is providing only a public key directory to find certificates. ICAO is **not** cerifying that the certificates are genuine. That is left to individual country certificate authorities [32, section 2.2.2]. However, if we consider an **active** third-party agent, this could be a secured computer owned by the passport holder's native country (or their consulate), but connected to the border control computer network. This way, any certificates that the passport chip inherently trusts (i.e., is already stored on-chip) can be used to verify the identity of the secured computer. If the passport chip can trust the secured computer [42], it can be assured that all its communications with the reader are fresh, i.e., it doesn't have to worry about keeping up-to-date with revocation lists. Note that the passport-issuing country does not need to sign an unlimited number of certificates. There are only about 200 countries in the world, and a given country might only allow a select set of other countries (such as the US Visa-Waiver countries) to have full access to the biometrics.

9 Visas

The ICAO proposals for MRTDs are currently for passports only, and they assume that the chip is written only by the issuing country and that other countries may not store data on the chip. This is necessary, partly because the current level of security available in smart card operating systems is not certified to protect national security against the threat of mutually-hostile applications. The Council of the European Union proposed [39] a biometric visa approach, in which each country affixed its own additional smart card chip in the passport at the time that the visa was issued to the passport holder. With a separate chip per visa-issuing country, there would be no need to provide the security required to permit multiple countries to write to the same smart card chip.

Unfortunately, as the EU investigated this approach to biometric visas, their study group determined [46] that storing multiple contactless smart card chips that close together in a single passport document resulted in a "collision" problem, when trying to read the contents of the chips. The typical contactless smart card reader that would be installed at a border crossing point would be unable to distinguish the communications of one chip from another. As a result, the EU is now considering that each country issue a visa on a smart card, separate from the passport. However, this would be significantly less convenient for the visa holder, and having multiple cards makes it more likely that some of them might be lost or stolen.

An alternate approach would be to use a smart card operating system that was sufficiently strong to permit multiple countries to download their own code and data onto the chip and still maintain security between them. Only two such smart card operating systems exist today. One is MULTOS, developed by Maos Corp. that has been evaluated [8] at the highest level (E6) of the European ITSEC evaluation criteria [24]. However, the evaluated configuration of MULTOS does not permit information sharing between applications which would make sharing data between the passport and the visa applications problematic. The only remaining possibility is the Caernarvon operating system [29] that is designed to be evaluated at the highest level (EAL7) of the Common Criteria [23]. Caernarvon includes a security model [43] to allow evaluated sharing of information between applications. However, Caernarvon is still only a research project and is not currently available as a product.[6]

The Caernarvon operating system can support electronic visas, because it includes a major extension to the traditional Bell and LaPadula [4] mandatory access control policy. This extension is called Multi-Organizational Access Classes, and it is described in more detail in [28] and in section 3 of [44].

The Bell and LaPadula secrecy model provides a lattice structure of nonhierarchic access classes. Each object in the system is assigned an access class, and each user is assigned a security clearance that is also an access class. Ac-

[6] The Caernarvon authentication protocol that was discussed in section 7 was developed for the Caernarvon operating system. However, the authentication protocol can also be implemented on conventional smart card operating systems. It does not depend on the rest of the Caernarvon system.

cess control decisions are made by comparing the access class of an object with the access class of the referencing user or process. The details of access classes are unimportant to this paper. What is important is that in a multi-organizational policy, the lattices may contain access classes from different mutually suspicious organizations, and that possession of these access classes can be strongly authenticated. Note that this type of multi-organizational access class is much more general than the access classes typically used in the US Department of Defense, such as those defined in the DoD Common Security Label [11].

Assume that there are three countries: a passport-issuing country P, a visa-issuing country V, and a third country Z. Country P has various treaty relationships with country V, but does not trust country Z at all. Each of these countries is assigned an organizational access class. The high-assurance Caernarvon operating system authenticates each potential reader, and as part of that authentication, determines to what access classes, the reader is allowed to have access. It also supports the downloading of evaluated *guard* processes that are permitted to re-mark information, but only in ways that were specified at the time of evaluation of the guard process and protected under a digital signature applied by the third-party evaluator.

The passport-issuing country P can provide some information to be shared read-only with the visa-issuing country V, and keep some information private. When the passport holder vists the embassy of country V to obtain a visa, the embassy will communicate electronically with country P to download onto the card a special guard process that is allowed to pass selected information from P to V, but is not allowed to change any other markings. Thus, the guard process would have no access to V's information, nor could it release information to country Z. Since the guard process belongs to country P, country P can ensure that it only releases appropriate informaton to V.

Similarly, each visa-issuing country can write its own data to the card, but not tamper with data belonging to any other country. By using combinations of organizational access classes and guard processes, one country could even share some data with some countries and other data with other countries.

If the passport holder wishes to obtain a visa for country Z, which the passport issuing country P does not trust at all, it is still possible, but country Z would not be able to store the visa on the passport chip, nor would country Z have access to the stored biometrics. Country Z could issue a separate document to the passport holder and collect its own biometric information, just as is done today for non-electronic passports.

10 Conclusion

A carefully planned and proper implementation of cryptographic and other security measures will undoubtedly improve the security of biometric passports and make them nearly impossible to forge with today's technology. However, ICAO's current plans for smart card-enabled biometric passports include some overly weak protection measures which can end up compromising the security and privacy measures that were meant to be enhanced with the new technology. We have shown how the current ICAO safeguards can be defeated in a number of ways with relatively low-cost technology. Armed with the information stolen from a passport, the criminal can carry out a variety of identity theft crimes, and worse still, an attacker could use the information to construct a false biometric credential that might then be used to exploit weaknesses in other biometric access control systems, such as those used to protect airfields, nuclear generating stations, and other critical infrastructure.

We have also shown alternate cryptographic techniques that could be used by ICAO to adequately protect the information on the passport chips without unduly raising deployment costs.

Going beyond biometric passports, we have also shown technical directions that could be taken to support the EU's desire for biometric visas by recommending new high assurance smart card operating system technology that could provide adequate security to allow multiple countries to safely write information to the same smart card chip.

Both the Kügler [34] and the Caernarvon [44] protocol focus on encryption to protect the biometric information on the smart card and when it must be transmitted to an authorized reader. However, there is current research underway to use the biometric as part of the cryptographic authentication protocol itself without revealing the biometric itself [7, 19, 50]. These new protocols have the potential to better protect the biometrics and to allow for revocation. They need to be seriously considered for future use for MRTDs.

11 Acknowledgements

This research was conducted while Gaurav S. Kc was a summer intern in the Internet Security and Technology Department at IBM T.J. Watson Research Labs in Hawthorne, NY. This report is based on publicly available material available at the ICAO/MRTD website, and standards from ISO/IEC and FIPS. We would like to thank the following people at IBM for lending their expertise and insights: Shai Halevi, Suzanne McIntosh, Elaine Palmer, Tal Rabin, Nalini Ratha, David Safford, Helmut Scherzer, David Toll, Wietse Venema, and Xiaolan Zhang. We also thank Dennis Kügler of the BSI in Germany for permission to cite his preliminary work.

Appendix: Grandmaster Chess Attack

Annex G of [32] describes the possibility that the passport could contain a special chip that actually communicates with a remote passport chip using some other network protocol, forwarding the border crossing point reader's messages to the other chip. This is called the "Grandmaster Chess Attack" [12, p. 75], but Annex G does not make clear how an attacker could gain benefit from such an attack.

Desmedt, Goutier, and Bengio [13] describe several attacks, based on the "Grandmaster Chess Attack", including "renting passports", and an attack useful to terrorist-sponsoring countries. Beth and Desmedt [5] propose solutions to these attacks, using highly synchronized clocks, but these solutions are impractical, because smart cards are not continuously powered nor do they include trustworthy clock functions. Anderson [2, pp. 19–20] describes a similar attack in a military IFF (Identify-Friend-or-Foe) system that he calls the "Mig-in-the-Middle-Attack". Alkassar, Stüble, and Sadeghi [1] also address these classes of frauds and suggest countermeasures based on probabalistic channel hopping to hide the conversation channel between users.

All of these frauds and protocols are based on purely cryptographic protocols and solutions. However, electronic passports have an advantage over these schemes — they have biometrics that can be checked against the human being who claims to be the passport holder. Even if the information is coming from a remote passport, it still must match the biometrics of the person at the border-crossing point. The biometrics and the human's identity will still be cryptographically bound together. Assuming that the biometric checks are strong and done securely, then it doesn't matter that the passport containing the digitally-signed biometrics is not present at the border.

Note that the assumption of strong and secure biometric checks is not necessarily valid. Facial images alone are not strong biometrics. Immigration officers, as well as automated facial recognition systems, will be easily fooled by identical twins or just people who resemble each other. Fingerprints and/or iris scans are likely to be more reliable, but as discussed in Section 5, the loss of such biometric information could assist in the creation of fake fingers.

In fact, the "Grandmaster Chess Attack" is a commonly used feature of many smart cards, where it is called "cryptographic tunneling". If a card holder wishes to use the card from home to perform internet commerce, the home computer would establish a cryptographic tunnel so that the smart card could securely communicate with some other server on the Internet. There is no easy way to distinguish legitimate uses of cryptographic tunnelling from what ICAO calls the "Grandmaster Chess Attack". For example, if the MRTD was also a national ID card, as proposed by a number of countries, such cryptographic tunneling a.k.a. "Grandmaster Chess Attacks" might be essential to using various government services over the Internet from home.

Annex G of [32] only says that the attack cannot be prevented. ICAO should update the annex to make clear which threats are of concern in a "Grandmaster Chess Attack" and discuss whether strong and secure biometrics could mitigate those threats acceptably. ICAO also needs to recognize that cryptographic tunneling could be an extremely useful feature for use of an MRTD as a national ID card.

References

1. Ammar Alkassar, Christian Stüble, and Ahmad-Reza Sadeghi. Secure object identification - or: Solving the chess grandmaster problem. In *Proceedings of the 2003 Workshop on New Security Paradigms*, pages 77–85, Ascona, Switzerland, 2003. ACM.
2. Ross Anderson. *Security Engineering – A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, New York, 2001.
3. Application interface for smart cards used as secure signature creation devices - part 1: Basic requirements. Technical Report CWA 14890-1, Comité Européen de Normalisation (CEN), Brussels, Belgium, March 2004. URL: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14890-01-2004-Mar.pdf.
4. David E. Bell and Leonard J. LaPadula. Computer security model: Unified exposition and multics interpretation. Technical Report ESD–TR–75–306, The MITRE Corporation, Bedford, MA, USA, HQ Electronic Systems Division, Hanscom AFB, MA, USA, June 1975.
5. Thomas Beth and Yvo Desmedt. Identification tokens - or: Solving the chess grandmaster problem. In *Advances in Cryptology - CRYPTO '90*, volume 537 of *Lecture Notes in Computer Science*, pages 169–176, Santa Barbara, CA, 1990. Springer–Verlag.
6. Biometrics deployment of machine readable travel documents. Technical Report ICAO TAG MRTD/NTWG Version 2.0, International Civil Aviation Organization, Montreal, QC, Canada, 21 May 2004. URL: http://www.icao.int/mrtd/download/technical.cfm.
7. Xavier Boyen, Yevgeniy Dodis, Jonathan Katz, Rafail Ostrovsky, and Adam Smith. Secure remote authentication using biometric data. In *Advances in Cryptology: EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 3494 of *Lecture Notes in Computer Science*, pages 147–163, Aarhus, Denmark, 22–26 May 2005. Springer–Verlag.
8. M. D. Brown. MULTOS version 4 on Hitachi AE45C integrated circuit card. Technical Report UK ITSEC Scheme Certification Report No. P167, UK IT Security Evaluation and Certification Scheme, Certification Body, Cheltenham, UK, June 2002. URL: http://www.cesg.gov.uk/site/iacs/itsec/media/certreps/CRP167.pdf.
9. Ran Canetti and Hugo Krawczyk. Security analysis of IKE's signature-based key-exchange protocol. In *Advances in Cryptology - Crypto 2002*, volume 2045 of *Lecture Notes in Computer Science*, pages 143–161, Santa Barbara, CA, 2002. Springer-Verlag.
10. David Clark. A proposed methodology for an ICAO PKI infrastructure for implementation of digital signatures on MRTDs. Technical Report Version 4, International Civil Aviation Organization, Montreal, Quebec, Canada, 19 April 2003.

11. Common security label (CSL). Technical Report MIL-STD-2045-48501, Joint Interoperability and Engineering Organization (JIEO), Fort Monmouth, NJ, 25 January 1995.
12. J. H. Conway. *On Numbers and Games*. Academic Press, London, 1976.
13. Yvo Desmedt, Claude Gouties, and Samy Bengio. Special uses and abuses of the fiat-shamir passport protocol. In *Advances in Cryptology - CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*, pages 21–39, Santa Barbara, CA, 16–20 August 1987. Springer–Verlag.
14. Development of a logical data structure (LDS) for optional capacity expansion technologies. Technical Report WD-006-2003-04-16, International Civil Aviation Organization, Montreal, Quebec, Canada, 16 April 2003.
15. Development of a logical data structure (LDS) for optional capacity expansion technologies. Technical Report LDS 1.7–2004–05-18, Revision 1.7, International Civil Aviation Organization, Montreal, Quebec, Canada, 18 May 2004. URL: http://www.icao.int/mrtd/download/technical.cfm.
16. Jon Edney and William A. Arbaugh. *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*. Addison-Wesley, Boston, MA, 2004.
17. Yair Frankel, Amir Herzberg, Paul A. Karger, Hugo Krawczyk, Charles A. Kunzinger, and Moti Yung. Security issues in a CDPD wireless network. *IEEE Personal Communications*, 2(4):16–27, August 1995.
18. Thomas C. Greene. US lubes passports with RFID snake oil. *The Register*, 20 May 2004. URL: http://www.theregister.co.uk/2004/05/20/us_passports/.
19. Feng Hao, Ross Anderson, and John Daugman. Combining cryptography with biometrics effectively. Technical Report UCAM-CL-TR-640, University of Cambridge Computer Laboratory, Cambridge, UK, July 2005. URL: (http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-640.html.
20. D. Harkins and D. Carrel. The internet key exchange (IKE). Technical Report RFC2409, November 1998. URL: ftp://ftp.rfc-editor.org/in-notes/rfc2409.txt.
21. Identification cards - contactless integrated circuit(s) cards - proximity cards - part 4: Transmission protocol. Technical Report ISO/IEC 14443-4, International Standards Organization, Geneva, Switzerland, 2000.
22. Identity cards bill. HL Bill 30, United Kingdom House of Lords, 21 February 2005. URL: http://www.publications.parliament.uk/pa/ld200405/ldbills/030/2005030.htm.
23. Information technology - security techniques – evaluation criteria for it security – parts 1, 2, and 3. Technical Report ISO/IEC 15408-1, -2, and -3, International Organization for Standardization, Genève, 1999.
24. Information technology security evaluation criteria (ITSEC). Technical Report Version 1.2, Commission of the European Communities, Brussels, Belgium, June 1991.
25. Philip Johnston. £70 ID card to combine passport and car licence. *The Daily Telegraph* (London, England), 4 July 2002. URL: http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2002/07/04/ncard04.xml.
26. Ari Juels, David Molnar, and David Wagner. Security and privacy issues in e-passports. In *SecureComm 2005, First International Conference on Security and Privacy for Emerging Areas in Communication Networks*, Athens, Greece, 5–9 September 2005. URL: http://www.cs.berkeley.edu/d̃aw/papers/epassports-sc05.pdf.
27. Dato' Mohd Jamal Kamdi. The Malaysian electronic passport. In *Twelfth Meeting of the Facilitation Division*, Cairo, Egypt, 22 March - 2 April 2004. International Civil Aviation Organization (ICAO). URL: http://www.icao.int/icao/en/atb/fal/fal12/presentations.htm.
28. Paul A. Karger. Multi-organizational mandatory access controls for commercial applications. Technical Report RC 21673 (97655), IBM Research Division, Thomas J.

Watson Research Center, Yorktown Heights, NY, 22 February 2000. URL: http://domino.watson.ibm.com/library/CyberDig.nsf/home.
29. Paul A. Karger, Vernon R. Austel, and David C. Toll. Using mandatory secrecy and integrity for business to business applications on mobile devices. In *Workshop on Innovations in Strong Access Control (WISAC)*, Naval Postgraduate School, Monterey, CA, 25–27 September 2000. URL: http://www.acsac.org/sac-tac/wisac00/wed0830.karger.pdf.
30. Paul A. Karger and Yair Frankel. Security and privacy threats to ITS. In *Proceedings of the Second World Congress on Intelligent Transport Systems '95 Yokohama*, volume V, pages 2452–2458, Yokohama, Japan, 9–11 November 1995. VERTIS: Vehicle, Road and Traffic Intelligence Society.
31. Ziv Kfir and Avishai Wool. Security and privacy issues in e-passports. In *First International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm 2005)*, pages 47–58, Athens, Greece, 5–9 September 2005. URL: http://eprint.iacr.org/2005/052.
32. Tom A. F. Kinneging. PKI for machine readable travel documents offering ICC read-only access. Technical Report Version 1.1, International Civil Aviation Organization, Montreal, Quebec, Canada, 1 October 2004. URL: http://www.icao.int/mrtd/download/technical.cfm.
33. Hugo Krawczyk. SIGMA: the 'SIGn-and-MAc' approach to authenticated diffie-hellman and its use in the IKE protocols. In *Advances in Cryptology – CRYPTO 2003 Proceesings*, volume 2729 of *Lecture Notes in Computer Science*, pages 399–424, Santa Barbara, CA, 17-21 August 2003. Springer–Verlag.
34. Dennis Kügler. Advanced security mechanisms for machine readable travel documents. Technical Report Version 0.90, Federal Office for Information Security (BSI), Bonn, Germany, 2005.
35. Susan Kumpf and Nora Russell. Getting the jump on fraud. *Cellular Business*, 9(10):24–26, October 1992.
36. Machine readable travel documents. part 1. - machine readable passports. Technical Report Document 9303, Part 1, International Civil Aviation Organization, Montreal, QC, Canada, March 2003.
37. Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. Impact of artificial "gummy" fingers on fingerprint systems. *Proceedings of the SPIE, Optical Security and Counterfeit Deterrence Techniques IV*, 4677:275–289, 24–25 January 2002. URL: http://cryptome.org/gummy.htm.
38. Naked data: How the U.S. ignored international concerns and pushed for radio chips in passports without security. American Civil Liberties Union, New York, 24 November 2004. URL: http://www.aclu.org/passports.
39. Presidency initiative on visa security and controls. Technical Report 10857/03, Council of the European Union, Brussels, Belgium, 24 June 2003. URL: http://www.statewatch.org/news/2004/dec/visas-presidency-paper-03.pdf.
40. RFID tags and contactless smart card technology: Comparing and contrasting applications and capabilities. Smart Card Alliance, Princeton Junction, NJ, 17 December 2004. URL: http://www.smartcardalliance.org/pdf/alliance_activities/rfidvscontactless_final_121704.pdf.
41. RFID tags, contactless smart card technology and electronic passports: Frequently asked questions. Smart Card Alliance, Princeton Junction, NJ, 3 January 2005. URL: http://www.smartcardalliance.org/pdf/alliance_activities/RFID_Contactless_Smart_Cards_FAQ_FINAL_010305.pdf.
42. Reiner Sailer, Xiaolan Zhang, Trent Jaeger, and Leendert van Doorn. Design and implementation of a TCG-based integrity measurement architecture. In *13th USENIX Security Symposium*, pages 223–238, San Diego, CA, 9–13 August 2004. USENIX Association. URL: http://www.usenix.org/publications/library/proceedings/sec04/tech/sailer.html.

43. Gerhard Schellhorn, Wolfgang Reif, Axel Schairer, Paul Karger, Vernon Austel, and David Toll. Verification of a formal security model for multiapplicative smart cards. In *6th European Symposium on Research in Computer Security (ESORICS 2000)*, pages 17–36, Toulouse, France, 4–6 October 2000. Lecture Notes in Computer Science, Vol. 1895, Springer Verlag.
44. Helmut Scherzer, Ran Canetti, Paul A. Karger, Hugo Krawczyk, Tal Rabin, and David C. Toll. Authenticating mandatory access controls and preserving privacy for a high-assurance smart card. In *8th European Symposium on Research in Computer Security (ESORICS 2003)*, pages 181–200, Gjøvik, Norway, 13–15 October 2003. Lecture Notes in Computer Science, Vol. 2808, Springer Verlag.
45. Bruce Schneier. Fatal flaw weakens RFID passports. *Wired News*, 3 November 2005. URL: http://www.wired.com/news/privacy/0,1848,69453,00.html.
46. Technical feasibility of the integration of biometric identifiers into the uniform format for visa and residence permits for third country nationals, passports and other travel documents issued by member states. Technical Report 14534/04, Council of the European Union, Brussels, Belgium, 11 November 2004. URL: http://www.statewatch.org/news/2004/dec/bio-visas.pdf.
47. Lisa Thalheim, Jan Krissler, and Peter-Michael Ziegler. Body check: Biometric access protection devices and their programs put to the test. *c't - magazin für computertechnik*, page 114, November 2002. URL: http://www.heise.de/ct/english/02/11/114/.
48. The Estonian id card and digital signature concept: Principles and solutions. AS Sertifitseerimiskeskus, Tallinn, Estonia, 5 June 2003. URL: http://www.id.ee/link.php/1038.
49. The identity project: An assessment of the UK identity cards bill & its implications. London School of Economics & Political Science, London, March 2005. URL: http://www.lse.ac.uk/collections/pressAndInformationOffice/PDF/IDreport.pdf.
50. Pim Tuyls, Anton H. M. Akkermans, Tom A. M. Kevenaar, Geert-Jan Schrijen, Asker M. Bazen, and Raymond N. J. Veldhuis. Practical biometric authentication with template protection. In *Audio- and Video-Based Biometric Person Authentication: 5th International Conference, AVBPA*, volume 3546 of *Lecture Notes in Computer Science*, pages 436–446, Rye Town, NY, 20–22 July 2005. Springer–Verlag.
51. United States, 107th Congress, second session. Enhanced border security and visa entry reform act of 2002. Public Law No. 107-173, 14 May 2002. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ173.107.pdf.
52. United States, 109th Congress. REAL ID act of 2005. Public Law No. 109-13, 11 May 2005. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ013.109.pdf.
53. United States Senate. Enhanced border security and visa entry reform act of 2001. *Congressional Record*, Daily Edition:S2643–S2659, 15 April 2002. URL: http://thomas.loc.gov/cgi-bin/query/C?r107:./temp/ r107YcVKwe.
54. Marc Witteman. Attacks on digital passports. In *What the Hack*, Liempde, near Den Bosch, The Netherlands. URL: http://wiki.whatthehack.org/index.php/Track:Attacks_on_Digital_Passports.
55. Junko Yoshida. Tests reveal e-passport security flaw. *Electronic Engineering Times*, (1336):1, 30 August 2004. URL: http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=45400010.
56. Kim Zetter. Feds rethinking RFID passport. *Wired News*, 26 April 2005. URL: http://www.wired.com/news/privacy/0,1848,67333,00.html.