Volume 8, No. 5, May – June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Enhancing the Security of E-Passports using a Secure Key Management Framework

Sadaf Abidin
Department of CSE, SEST
Jamia Hamdard, New Delhi, India

Abstract: E-passport or biometric passport is a hybrid document that combines paper format with electronic capabilities. They have been adopted by more than 45 countries to avoid counterfeiting of regular passports. MRTDs were introduced by the International Civil Aviation Organization (ICAO) in its Document 9303 which provides a set of rules and standards for e-passports. E-passports are based on the RFID technology, where the reader and the chip communicate through a wireless channel. Thus, an access control mechanism is necessary for privacy protection. In the early versions of e-passports, it was reported that various kind of security attacks was possible. BAC was proposed by ICAO and provides a mutual authentication and an encrypted communication channel between the IS and e-passport to prevent skimming and eavesdropping. In this paper, certain security weaknesses of e-passports have been discussed and their possible solutions are proposed. The Basic Access Control is also discussed in detail since it forms the basis for our proposed solution. Finally, we propose an alternative method for the generation and management of the initial access key (K_{seed}) which is input to the BAC algorithm.

Keywords: MRTDs, BAC, ICAO, Extended Access Control (EAC), Supplemental Access Control (SAC).

I. INTRODUCTION

E-passport or biometric passport is an electronic travel document that contains biometric information of the passport holder that can be automatically read and processed by a computer system to authenticate the citizenship of a person. It is a hybrid document that combines paper format with electronic capabilities. E-passports make use of two technologies: Radio Frequency Identification (RFID) and Biometrics. Today RFID technology is increasingly being used as an anti-counterfeiting tool in various application areas such as merchandise chains, personal identification and access control, financial credentials, sensor networks, etc. About 20 years ago, an official of the US national government had estimated that among the then 3 million US passport applications received every day at least 30,000–60,000 passports are fraudulent and only 1,000 fraudulent passports have been detected. According to the reports 80% illegal drug dealers and a large number of terrorists are aided with fake passports and visas and travel freely all over the world [1]. In order to improve the integrity of passport, the various countries have been issuing passports including a RFID chip that contains the passport holder's personal information. Malaysia was the first country in the world to issue e-passports in 1998, and till date, it has been implemented in more than 45 countries.

These machine-readable travel documents (MRTDs) were introduced by the International Civil Aviation Organization (ICAO) in its Document 9303 [2] which provides a set of rules and standards for e-passports. MRTDs are better than paper-based passports in terms of security and privacy since these are harder to forge and the passport holder cannot be easily impersonated. The aim of the ICAO is the secure authentication through documents that identify the owner of the document unambiguously.

Since e-passports are based on the RFID technology, an access control mechanism is necessary for privacy protection. In the early versions of e-passports, it was found that various kinds of security attacks were possible. In order to prevent skimming and eavesdropping the Basic Access Control security mechanism was proposed by ICAO. BAC uses symmetric-key cryptography and requires the key to be printed on the passport. Although it prevents skimming and eavesdropping, BAC offers very little privacy protection. Keeping these privacy issues into consideration, the EU introduced the Extended Access Control (EAC) which requires a public key infrastructure to be implemented for readers to protect the personal data in the RFID chip.

II. LITERATURE REVIEW

A considerable amount of research has already been conducted on Machine Readable Travel Documents (MRTD). One of the first security analyses on e-passports was presented by Juels, Molnar and Wagner [3] in 2005. Several drawbacks in the ICAO standard were identified by them which include clandestine scanning and tracking, biometric data leakage, eavesdropping, skimming and cloning. They also found certain defects in the cryptographic structure of the ICAO standard. Hoepman et al. [4] in 2006 discussed the passive attacks against Basic Access Control (BAC) and biometrics. The symmetric key between the reader and the chip has entropy less than 80 bits and can easily be guessed.

M. Lehtonen et al. [5] suggested in 2006 a possible solution against the clandestine reading and eavesdropping attacks by integrating the RFID enabled MRTD with the optical memory device. The communication channel between the reader and the optical memory device is secure since they require a line-of-sight connection for reading. The main drawback of this proposed idea is that a hardware change has to be done on passports.

V.K. N. Kumar et al. [6] suggested the on-line secure e-passport protocol provide mutual authentication between the inspection system and the e-passport. This protocol requires only the top level certificate issued by Country Verifying

Certificate Authorities (CVCA) to be stored in an e-Passport, which would reduce the memory requirements and prevent a Denial-of-Service attack by a malicious reader on an e-Passport. Although the current architecture of biometric passports provides good protection of biometric data of an individual, cloud computing could be used in the near future to perform a Brute Force Attack. A solution for this is to combine the cancellable biometrics with cryptographic protocols where the biometric data of a person can be protected by cryptographic keys that are exchanged by the Password-Authenticated Connection Establishment (PACE) protocol [7].

S. Kundra et al. [8] presented a paper in 2014 which mainly focuses on improving the security of e-passports using Biometrics. It presents a cryptographic security analysis of various technologies used in e-passport design specially using face fingerprint, palm print and iris biometric. These methods aim to provide improved security in protecting biometric information of the e-passport holder.

Antonia Rana et al. [9] in 2014 discussed the important aspects related to the management of keys and certificates issued by European Union Member States. They introduced two additional public key infrastructures that are required for the implementation of EAC namely EAC-PKI and single points of contact (SPOCs). EAC-PKI is used to manage the certificates needed to authenticate the terminals that access sensitive biometric information. SPOC controls the TLS protocol based secure channel between two endpoints which is necessary to exchange EAC-PKI certificates between two countries.

III. BASIC ACCESS CONTROL (BAC) PROTOCOL

To allow communication between the e-passport chip and the reader the ICAO has mandated the implementation of BAC in all e-passports. BAC is responsible for the key agreement and access control between the chip and reader. Actually, it was introduced to prevent skimming and eavesdropping and provide mutual authentication between the two devices.

Machine readable zone (MRZ) of the e-passport contains the information about passport holder. It includes name, country number, birth date and expiry date. This MRZ is scanned by the reader and information is recorded as input to BAC to create two triple-DES keys as shown in figure 1. After computing the keys K_{enc} and K_{mac} a three-pass challenge-response protocol is executed (figure 2).

The protocol begins with a challenge request sent by the reader. The tag responds with a 64-bit nonce (pseudo-random number). On reception, reader combines its random number with the tag's nonce and a 128-bit keying material generated by the reader.

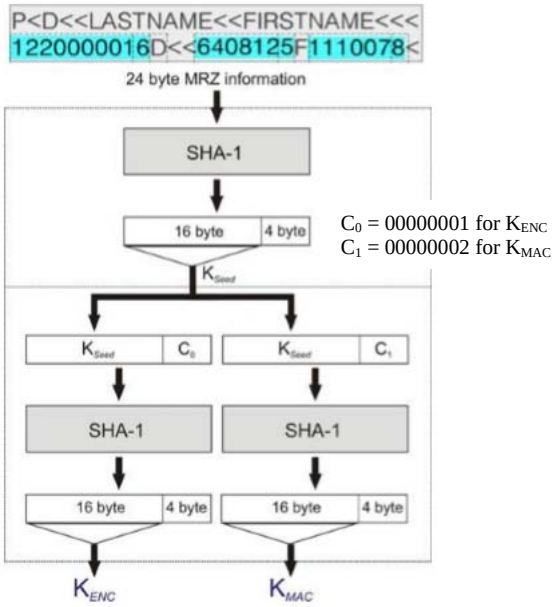

Figure 1: Derivation of BAC keys

Now, using the keys K_{enc} and K_{mac} ciphertext of the data and its checksum are computed and sent to the tag. Tag extracts and checks its nonce from the ciphertext and verifies the checksum. If the verification is successful, tag concatenates both the random numbers with its keying material and computes ciphertext. Tag sends the ciphertext and checksum to the reader. The validity of the checksum is verified by the reader and nonce is checked. If verified, the reader and the tag are considered to be mutually authenticated.

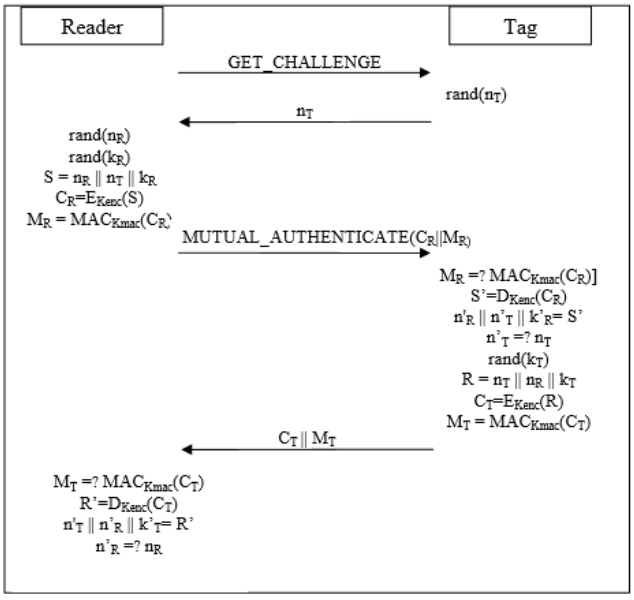

Figure 2: BAC three-pass challenge-response protocol

IV. PROBLEM STATEMENT

An issue for the BAC mechanism comes from the fact that the access key seed (K_{seed}) used in the BAC is a fixed key which is directly obtained from the static Machine Readable Zone (MRZ) information. K_{seed} is used to derive the encryption key K_{ENC} and the MAC computation key K_{MAC}. These keys are then used for mutual authentication between the reader and the passport chip. Once an inspection system

at a border office (or hotel) has access to the information in the MRZ zone, the BAC key is known for the lifetime of the passport. That means these keys can be used to access the passport data till the validity of the passport. Access to the passport data protected under BAC is irrevocable. If an attacker successfully recovers the K_{seed} by executing a Brute Force attack, following security objectives will not be fulfilled: Mutual authentication, Data confidentiality and Forward secrecy.

The main problem lies in the key derivation process up to obtaining K_{seed}. The data fields on the passport are static and have a limited range of values. These can be guessed by an attacker with basic information about the victim. Consequently, the attacker might use this data for the generation of the keys which is a notable security issue. Therefore, to resolve this issue, a secure K_{seed} derivation process has been proposed.

V. PROPOSED SOLUTION

A method for the generation and management of the initial dynamic access key has been proposed which is based on the client-server model. According to the solution, the access keys will be computed every time the e-passport is scanned by the reader and authenticated. At the time of issuing the passport, the key can be generated from random data. Then, instead of the key itself, the key ID is stored in the e-passport.

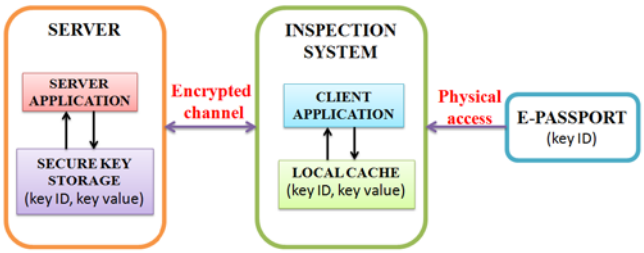

Figure 3: Components of the access key framework

The proposed model for key generation and management consists of five main components (Figure 3):

1. **E-passport**: It contains the chip where the personal information of the passport holder is stored and a key ID is either printed on the passport or stored within the chip. This key ID will be used by the inspection system at the time of verification.
2. **Inspection system (IS)**: The client application is installed in the IS which interacts with the server for accessing keys. The IS also consists of a high speed local cache.
3. **Server**: It consists of the server application that communicates with the client and processes the key requests. Server is attached to a secure storage that stores the keys. The main function of the server is to authenticate the client whenever an inspection system tries to connect to the server for accessing the keys. Keys are computed at the server.
4. **Local Cache**: It is incorporated within the IS (client module) and stores previously used keys.
5. **Secure key storage**: The database that stores the key values associated with the key Ids contained in the e-passport. The key values are required to be digitally signed before storage and verified upon retrieval to ensure integrity.

Working of the system is diagrammatically explained in figure 4. The steps are as follows:

- IS gets the key ID by scanning the e-passport.
- IS sends the key request to the client module that resides in it.
- Once the key request arrives at the client, the key values are searched within the local cache which is integrated in the client module.
- If the key value is found in cache it is sent to the IS application. IS can then use these key values for further validation process.
- If the values are not found in the cache then the client module is required to retrieve the values from the server.
- A secure (encrypted) communication channel is established between the client and the server after the client authenticates itself to the server.
- The main aim of the server is to authenticate the IS (client application) and then process the key request after all the security policies are fulfilled.
- Key requests can be of two types- key retrieve or new key. The server can process the requests in two ways:
  Key retrieve: Server extracts the key values associated with the key ID from the key storage and forwards it to the IS.
  New key: New keys are computed at the server according to the information specified by the IS in the request and updated on the key storage.
- After all the requests have been processed the required key or an error message is sent back to the IS client.

VI. DISCUSSIONS

The explained framework is observed to be more secure than the fixed access key infrastructure. The system should fulfil certain requirements in order to prevent it against attacks. It is necessary that only the authorized clients connect to the server for accessing keys. For this an access control mechanism is required to be established to the server. It can be done by using digital signature certificates between the client and the server. The client-server communication channel must be secure (encrypted) in order to avoid a passive listener from eavesdropping. That means the key requests from the client side and the responses from the server must be encrypted prior to transmission. The database records in the key storage should be digitally signed before they are stored and upon retrieval they can be verified to ensure integrity of the data. In this way any modification done by an attacker can be detected and the client can be notified accordingly. Moreover, the keys in the database should be encrypted before storage in order to prevent an attacker from accessing the keys thus ensuring data confidentiality. The advantages of variable access key over fixed access key can be summarized in Table 1.

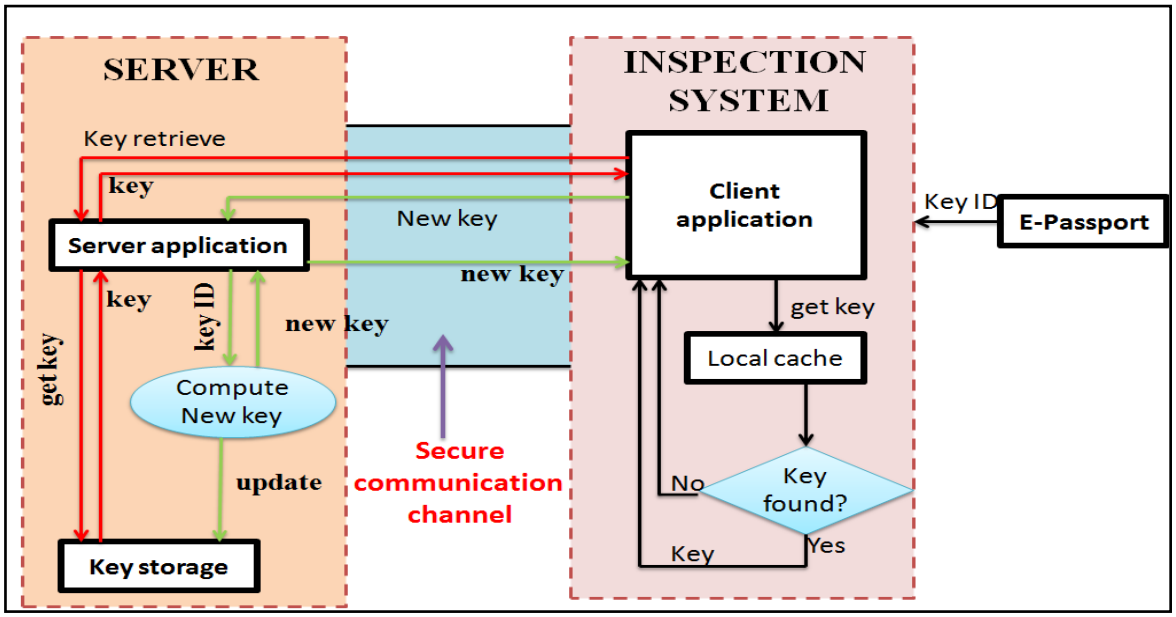

Figure 4: Working of the system

The RFID chip within the e-passport can actually be read by the reader from up to a distance of 30 feet [10]. Attackers may set up hidden unauthorized readers of a similar nature to gain access to the information being transmitted by the readers thus affecting their integrity. A possible solution to prevent the chip from responding to an unauthorised intruder could be placing document in a faraday cage or adding a switch (or a sensor) to e-passport such that the passport can be switched off when not in use.

BAC makes use of the SHA-1 (Secure Hash Algorithm 1) to open secure messaging. SHA-1 takes 24 bytes of MRZ information and produces a 20 byte output which is then used for obtaining the K_{seed} and subsequent keys. On February 23, 2017 Google announced they had performed a collision attack against SHA-1 publishing two different PDF files which generate the same SHA-1 hash. Therefore, any other secure hashing algorithm should be used instead of the SHA-1. Many organizations have recommended the use of SHA-2 or SHA-3 instead of SHA-1.

Table 1: Advantages of dynamic access keys

S. NO.	*BASIS FOR DISTINCTION*	*FIXED ACCESS KEY*	*DYNAMIC ACCESS KEY (proposed system)*
1.	**Origin of access key**	Generated from static MRZ information.	Generated by using some random data.
2.	**Storage**	Access keys are either stored in the chip or printed on the passport.	Access keys are stored in the secure server storage and Key ID is stored in the e-passport.
3.	**Validity of key**	Lifetime of the document (validity of the e-passport).	Valid for a limited time period (depends upon implementation).
4.	**Possibility of attack**	High. If an attacker gets the key then access to the passport data is irrevocable.	Low. If an attacker gets the key ID, in order to get the key values he will have to be authenticated to the server first.

VII. CONCLUSION

In this paper, we have analyzed one of the notable weaknesses of the Basic Access Control keys (fixed initial access key) implemented in electronic passports and proposed the key management framework as a solution to the problem stated. Although the proposed idea solves the shortcomings of the conventional BAC protocol, it is somewhat complex to be implemented. However, the idea can be used in other electronic documents like enhanced driving license and PASS cards. In addition to BAC which is made mandatory by the European Union (EU) harder access control mechanisms viz. Extended Access Control

(EAC) and Supplemental Access Control (SAC) have been launched by the ICAO which are based on public key cryptography. EAC was introduced to protect sensitive biometric data like the fingerprint. SAC has been added as a supplement to BAC and EAC. These protocols require high-cost IC chips. The major barrier to the global acceptance and implementation of biometric passports is the inconsistency in privacy laws among different countries.

REFERENCES

1. B. King, X. Zhang, RFID: An Anti-counterfeiting Tool. RFID Security: Techniques, Protocols and System-On-Chip Design. Springer Science+Business Media, LLC 2008.
2. ICAO Doc 9303, Machine Readable Travel Documents, Seventh Edition 2015, Part 3: Specifications common to all MRTDs.
3. A. Juels, D. Molnar, D. Wagner. Security and Privacy Issues in E-Passports. In Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05), Washington, DC, USA, pp. 74–88, IEEE, 2005.
4. J.-H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, R. Wichers Schreur. Crossing Borders: Security and Privacy Issues of the European e-Passport. In Advances in Information and Computer Security, First International Workshop on Security (IWSEC'06), Kyoto, Japan, Lecture Notes in Computer Science 4266, pp. 152–167, Springer-Verlag, 2006.
5. M. Lehtonen, T. Staake, F. Michahelles, E. Fleisch. Strengthening the Security of Machine Readable Documents by Combining RFID and Optical Memory Devices. Presented at Developing Ambient Intelligence: Proceedings of the First International Conference on Ambient Intelligence Development (Amid'06), 2006, Sophia Antipolis, France, pp. 253–267, Springer, 2006. to appear in International Journal of Information Security (IJIS).
6. V.K. N. Kumar, B. Srinivasan. Design and development of e-passports using Biometric access control system. International Journal Of Advanced Smart Sensor Network Systems (IJASSN), Vol 2, No.3, July 2012.
7. Rima Belguechi, Patrick Lacharme, Christophe Rosenberger. Enhancing the privacy of electronic passports. International Journal of Information Technology and Management (IJITM) Special Issue on: "Advances and Trends in Biometrics".11 (1/2), pp.122-137, 2012
8. S. Kundra, A. Dureja, R. Bhatnagar. The Study of recent technologies used in E-passport system. IEEE Global Humanitarian Technology Conference - South Asia Satellite (GHTC-SAS), September 26-27, 2014.
9. A. Rana, L. Sportiello. Implementation of security and privacy in e-Passports and the extended access control infrastructure. International Journal of Critical Infrastructure Protection 7 (2014) 233-243.
10. Gonsalves, C. 2005. A Ticket to Trouble; RFID-enabled passports pose privacy, security risks. eWeek. 2005, Vol. 22, 19, p. 33.