Security and Performance Evaluation Platform of Biometric Match On Card

Benoît Vibert, Alexandre Ninassi, Christophe Rosenberger

Security and Performance Evaluation Platform of Biometric Match On Card

Benoit Vibert, Christophe Rosenberger

Normandie Univ, France;
UNICAEN, GREYC F-14032 Caen, France;
ENSICAEN, GREYC, F-14032 Caen, France;
CNRS, UMR 6072, F-14032 Caen, France
{*benoit.vibert,christophe.rosenberger*}*@ensicaen.fr*

Alexandre Ninassi

TazTag
Bruz, France;
alexandre.ninassi@taztag.com

***Abstract*—In order to verify the identity of a cardholder user, the typing of a PIN code is usually required, but this method does not guarantee the verification result. Only biometrics is able to authenticate an user as this information is strongly related to the user. To ensure security and privacy issues (such as the protection of the biometric data), Match On Card (MOC) solutions have been proposed. This approach consists in storing the biometric user's reference and computing the verification decision in a Secure Element (SE). The purpose of this paper is to propose an evaluation platform on biometric MOC for testing its performance and security. This platform allows to perform tests given scenarios and benchmarks for comparing MOCs. We illustrate the usefulness of this platform on a commercial MOC.**

I. Introduction

Biometric systems are increasingly used to check or determine the identity of an individual. Their main uses are related to the areas of border control, physical access control or electronic commerce. These applications may require the use of large online biometric databases but it can cause many security and privacy problems. In order to avoid these problems, storage and Match On Card (MOC) for biometric verification are increasingly made on a Secure Element (SE) as the French passport chip. The main benefit of this solution is to avoid the transmission of the biometric reference of the user. The user has also the control of its own biometric data stored in the SE. A secure element guarantees many security issues of the biometric reference (confidentiality, integrity).

Given the issues related to the use of SE for several applications such as border control or face to face bank payment, it becomes very important to define a general methodology for evaluating these embedded systems. The objective of this paper is to propose an evaluation platform of biometric MOC for analyzing its performance and security.

The paper is organized as follows. Section 2 is devoted to the state of the art on the evaluation of biometric systems and MOC based ones. Section 3 describes the proposed platform. In Section 4, we illustrate the benefit of the proposed platform through experimental results on a commercial MOC. We conclude and give some perspectives on this work in Section 5.

II. State of the art

In this section, We first give some generalities of biometric systems. We also present the different evaluation methods of a biometric system: quality of biometric data, performance, security and usability. We describe the different existing benchmark databases that can be used for the evaluation task of biometric systems. Finally, we present the existing platforms for testing and characterizing MOC based biometric systems.

A. Generalities on biometric systems

The aim of biometric systems is to verify the identity of an entity which access to a resource. In the case of physical access, this resource can be a building or a room, whereas in the case of logical access, this resource can be an application on a computer. Different biometric modalities can be classified among three main families (even though we can find slightly different characteristics in the literature like the biological one that is often forgotten):

- Biological: recognition based on the analysis of biological data linked to an individual (e.g., DNA, EEG analysis, .).
- Behavioral: based on the analysis of an individual behavior while performing a specific task (e.g., keystroke dynamics, signature dynamics, gait, .).
- Morphological: based on the recognition of different physical patterns, which are, in general, permanent and unique (e.g., fingerprint, face recognition, .).

Biometric authentication systems are generally composed of two main modules: (a) the enrollment module which consists in creating a template (or reference) for the user with the help of one or several biometric captures (or samples), and (b) the verification module which consists in verifying if the provided sample belongs to the claimed user by comparing it with its template. After verification, a decision is taken to decide to accept or to reject the user depending on the result of the comparison.

B. Evaluation methods

In a complete biometric system, we can evaluate each part to quantify its impact on the final result. As for example, a poor fingerprint quality can affect the performance of the system. The evaluation of a complete biometric system is based on several criteria.

1) The quality of the captured biometric data: In the literature, we find many elements that addresses the quality of the fingerprints [5]. As for example, Alonso-Fernandez and *al.* [6] presented an overview of existing methods to quantify the quality of fingerprints. The authors show the impact of poor image quality on the overall performance of biometric systems. Other methods for measuring the quality of the fingerprints are given in [8], [9]. These methods have proved effective in predicting the quality of fingerprint images. NFIQ metric proposed by NIST is now the reference for this task and is part of all industrial sensors SDK fingerprint [7].

2) Performance: We intend here to measure the efficiency of a biometric system in terms of recognition errors in a given context of use. It is quantified by statistical measures (error rate, processing time, etc.). The measures proposed by the International Organization for Standardization ISO/IEC 19795-1 [1] to evaluate and compare the performance of biometric systems are effective and comprehensive.

3) Security: With regard to security, a biometric MOC uses two technologies: biometrics and smartcard. This implies that the MOC have vulnerabilities resulting from its origins, we quickly present them. For the biometric part, Ratha and *al.* [11] have combined attacks of a generic biometric system in 8 classes (falsified biometric data, interception of biometric data during its transmission, attack on the extraction module parameters, altered extracted parameters, matching module replaced by a malicious software, alteration of the database, man in the middle attack between the database and the matching module and alteration of the verification decision). For each point, there are different types of attacks. Figure 1 illustrates the possible locations of the attacks in a generic biometric system.

Smart cards are sensitive to three types of classical attack: invasive, semi-invasive and non-invasive. With regard to the invasive and semi-invasive attacks, they are performed after removing the micro-processor from the socket and having removed the resin layer covering it. We can make microprobing [12], ion bombardment [12]. For the non-invasive approaches, it is possible to perform fault injection attacks [15] or side channel attacks such as execution time [13], or power consumption SPA (Single Power Analysis) [14], DPA (Differential Power Analysis) [15]. The smartcards can also be sensitive to man-in-the-middle attacks, such as the Cambridge one [16]. We have seen briefly the different types of attacks which exist both for biometric systems and smartcard, it is necessary to evaluate their effectiveness in the context of a biometric MOC.

4) Usability: This evaluation aspect is to analyze the user perception of the system and to quantify its satisfaction and acceptability. The work presented by El-Abed et *al.* [18], Jain and *al.* [19], Kukula and Proctor [20] and Kubula and *al.* [21] show the importance of this evaluation in the design and comparison of biometric systems [20]. An effective system in terms of performance but not acceptable, is not considered interesting (as in the case of DNA verification systems for physical access control).

C. Benchmark

To evaluate biometric systems, it is necessary to have a database containing biometric data. This database ensures that the systems are tested under the same conditions and allows for reproducible results to compare biometric MOC. Examples of biometric databases from research competitions are FVC2002 or FVC2004 [22], [23]. Moreover, it is also interesting to perform tests of the same MOC when we use multiple databases acquired under different conditions (biometric sensor, population, environment, etc.). It is also necessary to define test scenarios (number of biometric data for enrollment, number of data for testing ...).

D. Platforms

With regard to platforms, there are quite a few in the literature. We can already cite the NIST platform [2], which is used in their annual research competitions. It allows manufacturers to test their MOC or minutiae extractors, in terms of interoperability. In the NIST report, information on FAR (False Acceptance Rate) and FRR (False Rejected Rate) rates for every MOC and different extractors are disseminated.

We can also mention the online FVC-Ongoing platform [3] dedicated to algorithms for fingerprint verification (evolution of the FCV competitions). The platform offers multiple databases grouped into two parts. The first one (Fingerprint Verification) quantifies both enrollment and verification modules, while the second one (ISO Fingerprint Matching) quantifies only the verification module on ISO Templates [4] based on minutiae. Performance metrics are: the failure to acquire rate (FTA) and the failure to enroll rate (FTE), the false non match rate (FNMR) for a defined false match rate and vice versa, the average enrollment and verification times, the maximum size required to store the biometric template on the SE, the distribution of legitimate and impostors users scores and the ROC curve with the associated equal error rate (EER). The main drawback of this platform is that it is necessary to submit the executable or source code of the MOC to the online platform which can cause confidentiality issues.

E. Discussion

The evaluation of biometric verification algorithms is most of time used during the algorithm prototyping by researchers

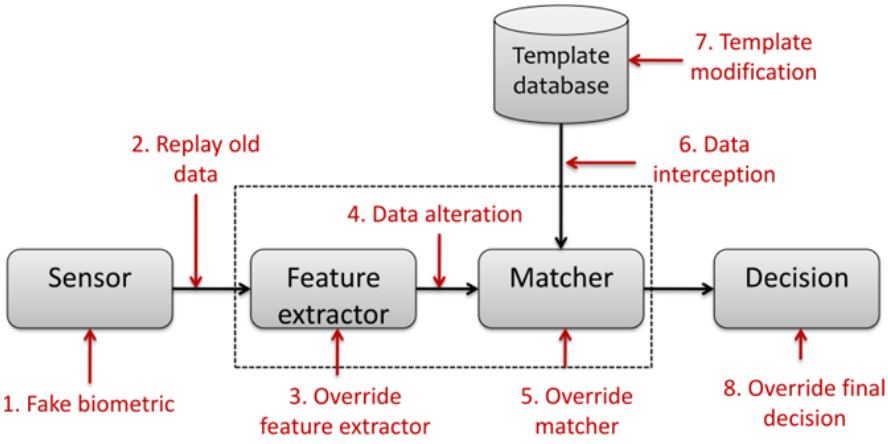

Fig. 1. Vulnerabilities locations of a biometric system (extracted from [11])

and relatively little by the industrial world. The evaluation methods and platforms fail to satisfy all of our needs. We intend to realize security analysis of a research or a commercial biometric MOC, to measure performance in terms of errors or verification average time.

III. Platform Architecture

The general synopsis of the proposed platform is given Figure 2). It permits to make different types of classical analysis of literature but also more advanced aspects including security. For example, the platform allows to make gray and white box tests of the implementation of a biometric MOC. This will allow developers to have information on the MOC implementation in order to optimize it. The proposed platform is composed of several modules that we will define in the next section.

A. Modules

The platform is made up of different modules allowing to make specific treatments, such as the interface to connect biometric databases. The central element is the `Core`, all other modules have no knowledge on others. This allows to modify a module without changing the overall operation of the platform. All modules are independent, we can change one and then see the effect of this change on the results. This will allow us, for example, to quantify the impact of a biometric database on the results or if an algorithm is better than another. The proposed platform uses active mechanisms of communication by event allowing multiple modules simultaneously access data exchanged between the client application and the MOC, thus offering the possibility of analyzing ”on the fly” results.

1) Core: The `Core` is the main module that interfaces and manages all modules. It orchestrates the interaction with the different modules. It only knows the type of data as input of the MOC and the type of data returned by the MOC. As for example, to communicate with the Secure Element, the `Core` transparently manages the connection and communication with the MOC, it is realized by Personal Computer/Smart Card (PCSC) communication [10] or Java Card OpenPlatform (JCOP) simulator with the software library developed through WSCT in [17].

2) Database Interface: The module `Interface` manages all biometric databases. The `Core` requests to the interface the next biometric data for processing and delegates to the interface the connection and management of all biometric databases. This allows to abstract the storage format of biometric data for example.

3) Scenario: The module `Scenario` permits to create or use an evaluation scenario. It defines the biometric database to query, the number of biometric data to be used for enrollment or the number of users to consider. This allows us to make reproducible testing only by setting these elements. The module `Performance` quantifies the impact of these changes.

4) Performance: This module allows to evaluate the performance of the MOC with different metrics: FAR, FRR, EER, NIFQ value of each capture, ROC curve, enrollment and verification time. It also allows us to save the results in a database to compare several MOC based on the same test scenario.

5) Security: This module contains various attacks on the MOC. It is possible to use fuzzing approaches [24] consisting in injecting fault data to the biometric MOC. It can be a biometric template respecting the ISO format but containing random biometric data (brute force attack). It is also possible to test the interoperability of the MOC by providing biometric templates ISO in which faults have been injected.

6) GUI Interface: The proposed platform has a main graphical interface that allows to choose the test scenario and evaluation metrics. From the main interface, you have the option of using ”plugins” that allow us to get informa-

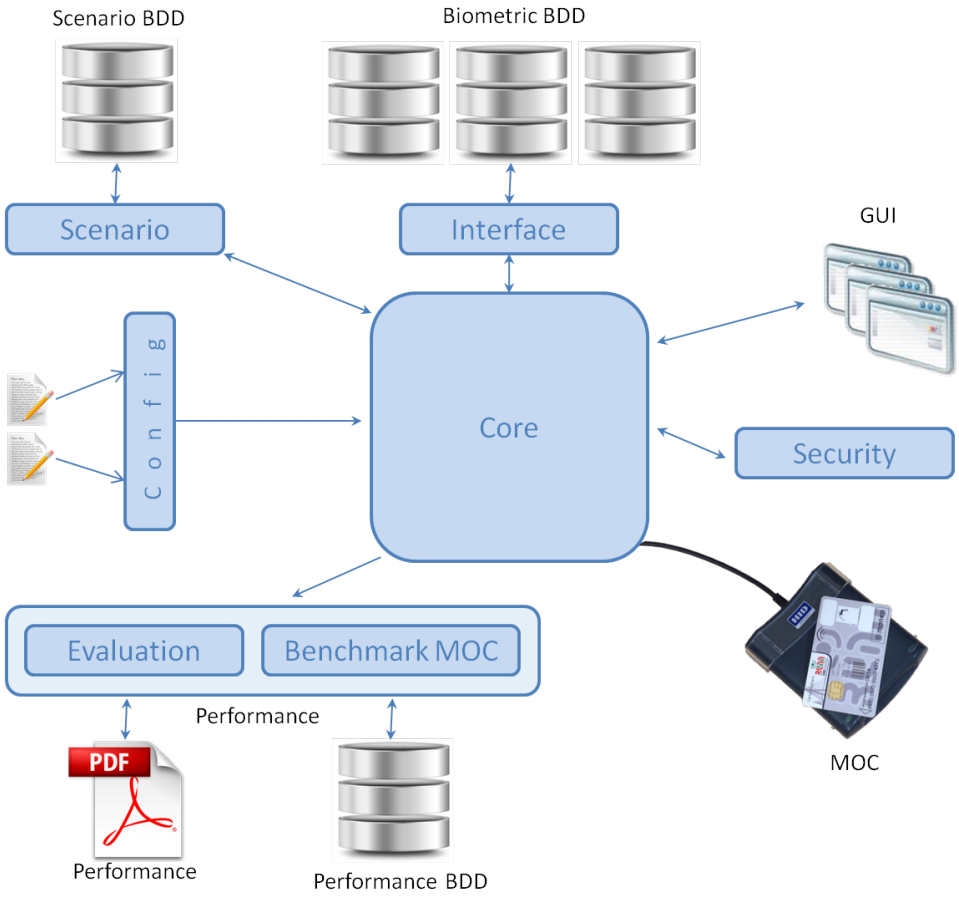

Fig. 2. General schema of the platform

tion about one or more elements (eg minimum, average and maximum time for enrollment and verification). As mentioned earlier, the proposed platform uses active communication by event mechanisms, which provides access to information that you want in just developing a plugin that allows to visualize evaluation results as for example.

B. Evaluation metrics

As a first step, we use classical metrics commonly used in the literature and more specific ones:

- False Acceptance Rate (FAR): it measures how many times the biometric data of a user provides positive verifications with biometric data of another user.
- False Rejection Rate (FRR): it measures how many times the biometric data of a user gives a negative verification of biometric data with the same user,
- Success rate of attack: it measures the ratio of successful attacks (number of positive result over a number of transactions).
- Measuring interoperability: it quantifies the ratio of successful tests when providing an ISO template to the MOC.
- ROC curve: It describes the behavior of the biometric MOC for each value of the decision threshold (from which a test is positive). This implies that it is possible to obtain the comparison score from the MOC or to set decision threshold. For industrial MOCs, this is rarely the case but for research ones, this information is always available.
- Verification Time: we measure the time required to achieve a MOC enrollment or to obtain a verification result (after sending the ADPU (Application Data Protocol Unit defined in [25]) to the SE. It is also possible to generate several statistics on computation times such as histogram verification time, average, minimum or maximum time.
- Correlation between verification time and score : In general, a positive verification is slower than a negative one. This information can be exploited by an attacker as it can analyze the response time for the MOC to identify the extent to where the transmitted data is near the biometric reference stored on the SE (approach called Hill Climbing attack in the literature [26]). In order to quantify if a MOC could be attacked by the Hill climbing attack, we measure the Pearson correlation factor between the verification time and score returned by the MOC (when known). A strong correlation highlights a flaw in the biometric MOC, as indication the template is similar to the reference if the

time decrease.

IV. Experimental results

We illustrate the benefit of the proposed platform on a commercial MOC (we do not name). We explain the protocol we used for the experiments and we study the performance we obtained for this MOC.

A. Protocol

The biometric data we use have been collected in an earlier study involving 39 individuals. Three captures sessions have been conducted with two fingers: left index finger and right index finger (*cf.* Figure 3), with 5 captures per session and per person. In this study, 1170 ($3 \times 5 \times 39 \times 2$) fingerprint images have been captured.

Fig. 3. Example of fingerprint capture *(left and right index)*

To ensure maximal interoperability, the data exchanged are stored in the compact ISO standard (in the form of a string of bytes: each byte is represented in hexadecimal value).

B. Performance

We use the first of the 15 captures of an individual as enrollment template. For intra-class results (comparison of fingerprints from the same person), we compare each user's biometric reference with the 14 other captures (template verification). (*cf.* Figure 4) gives an example of verification results (MOC_OK: postive verification or MOC_NOK: negative verification) and verification time. For example, the first comparison is performed in 1.145 seconds.

With regard to the inter-class results (comparison of fingerprints of different individuals), we compared the biometric reference of a user with all fingerprints from other individuals (template verification). Figure 5 gives some examples of interclass comparisons with the associated verification time.

We computed $14 \times 38 = 532$ intra-class and $14 \times 38 \times 39 = 20748$ inter-class scores. From these data, we can calculate many performance metrics. For example, for the left index finger, we got a FAR of 0.417% and FRR of 17.36%. To the

```
OUT ==> MOC(E000/V002)=0 MOC_OK      00:00:01,145
OUT ==> MOC(E000/V003)=1 MOC_NOK     00:00:03,524
OUT ==> MOC(E000/V004)=0 MOC_OK      00:00:02,362
OUT ==> MOC(E000/V005)=1 MOC_NOK     00:00:02,550
OUT ==> MOC(E000/V006)=1 MOC_NOK     00:00:00,719
OUT ==> MOC(E000/V007)=0 MOC_OK      00:00:01,330
OUT ==> MOC(E000/V008)=1 MOC_NOK     00:00:00,250
OUT ==> MOC(E000/V009)=0 MOC_OK      00:00:01,502
OUT ==> MOC(E000/V010)=1 MOC_NOK     00:00:00,375
OUT ==> MOC(E000/V011)=1 MOC_NOK     00:00:02,597
OUT ==> MOC(E000/V012)=0 MOC_OK      00:00:02,878
OUT ==> MOC(E000/V013)=0 MOC_OK      00:00:02,300
OUT ==> MOC(E000/V014)=1 MOC_NOK     00:00:02,112
```

Fig. 4. Intra-class performance scores (comparison of the biometric data from the same individual)

```
OUT ==> MOC(E000/V015)=1 MOC_NOK     00:00:01,892
OUT ==> MOC(E000/V016)=1 MOC_NOK     00:00:01,862
OUT ==> MOC(E000/V017)=1 MOC_NOK     00:00:01,768
OUT ==> MOC(E000/V018)=1 MOC_NOK     00:00:01,955
OUT ==> MOC(E000/V019)=1 MOC_NOK     00:00:02,315
OUT ==> MOC(E000/V020)=1 MOC_NOK     00:00:01,377
OUT ==> MOC(E000/V021)=1 MOC_NOK     00:00:01,157
OUT ==> MOC(E000/V022)=1 MOC_NOK     00:00:01,252
OUT ==> MOC(E000/V023)=1 MOC_NOK     00:00:01,877
OUT ==> MOC(E000/V024)=1 MOC_NOK     00:00:01,423
```

Fig. 5. Inter-class results scores (comparison of the biometric data from different individuals)

right index finger, we have a FAR of 0.283% and FRR of 17.79%. As a conclusion of the performance, there is a fairly good robustness to imposture but a too high FRR value(17%).

C. Time

The verification time is an average of 1.3 seconds. The sample (*cf.* Figure 6) relates 5645 observed time transactions for 10 individuals.

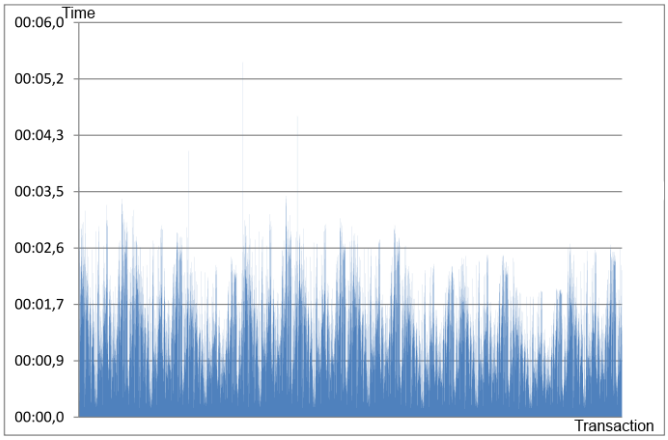

Fig. 6. Sample time of enrollment and verification

Minimal verification time is 0.5 seconds and the maximal

one is 5.5 seconds. The maximal time is not acceptable in a banking transaction as for example.

D. Discussion

We observed quite satisfactory performance in terms of verification time and false acceptance rate compared to those found in [2]. Nevertheless, the false rejection rate is too high, several factors explain that.

The choice of the template enrollment was made from a list of captures without any selection. No quality control of the capture (with the NFIQ metric as for example) or consolidation of the template by a specific function for the enrollment step has been made. Figure 7, show some poor quality captures in the database. The calculate NFIQ average is 2.59. The pourcentage for each NFIQ value is 1.33% for $NFIQ = 1$, 33.33% for $NFIQ = 2$, 34.66% for $NFIQ = 3$, 22.62% for $NFIQ = 4$ and 8% for $NFIQ = 5$. This explains the results. We plan to use this platform to compare the relative performance of MOC on the same biometric data (known benchmark from the literature such as those used at FVC2002 and FVC2004 competitions) and following the same protocol.

Fig. 7. Capture images of poor quality

It is possible to improve the performance of the MOC by performing an enrollment with a quality control of the fingerprint but this defines another test scenario. Thanks to this platform, it could be tested very easily by defining another scenario consisting in adding a new step during the enrollment step.

V. Conclusion and perspectives

We proposed in this paper an evaluation platform of biometric MOC. It allows to test some aspects of security and performance. Its modular architecture allows simple evolution by integrating new attacks or metrics. It is very easy to adapt the analysis of a MOC through xml files. We illustrate how it works on a few points on a commercial MOC.

The perspectives of this work include the development of additional modules to enrich the test scenarios as the pre-processing biometric template (selection of the most relevant minutiae as for example). It is also possible to define methods of complex attacks to test the robustness of biometric MOC.

References

[1] ISO/IEC 19795-1. Information technology - biometric performance testing and reporting - part 1 : Principles and framework, 2006.

[2] P. Grother, W. Salamon, C. Watson, M. Indovina, and P. Flanagan, MINEX II “Performance of Fingerprint Match-on-Card Algorithms” Phase IV : Report NIST Interagency Report 7477 (Revision II), 2011.

[3] https://biolab.csr.unibo.it/FVCOnGoing

[4] ISO/IEC 19795-2. Information technology - biometric data interchange format - part 2 : Finger minutiae data, 2004.

[5] M. El Abed, B. Hemery, C. Charrier, and C. Rosenberger. ”Evaluation de la qualit de donnes biomtriques”. Revue des Nouvelles Technologies de l’Information (RNTI), numro spcial ”Qualit des Donnes et des Connaissances / Evaluation des mthodes d’Extraction de Connaissances dans les Donnes”, p.1-18, 2011.

[6] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K.Kollreider, and J. Bigun. ”A comparative study of fingerprint image-quality estimation methods”. IEEE Transactions on Information Forensics and Security, vol. 2 : p. 734-743, 2007.

[7] E. Tabassi, C. L. Wilson, A novel approach to fingerprint image quality. In IEEE International Conference on Image Processing, (ICIP), volume 2, pp. II-37, 2005.

[8] P. Grother, E. Tabassi, Performance of biometric quality measures. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 4, number 29, p. 531-543, 2007.

[9] S. Lee, C. Lee, and J. Kim. ”Model-based quality estimation of fingerprint images”. In IAPR/IEEE International Conference on Biometrics (ICB’06), p. 229-235, 2006.

[10] PC/SC Workgroup Specification 2, PC/SC Workgroup, http://pcscworkgroup.com/, 2005

[11] N.K. Ratha, J.H. Connell, and R.M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, vol. 40 : p. 614 - 634, 2001.

[12] Oliver Kmmerling and Markus G. Kuhn. Design principles for tamper-resistant smartcard processors. p. 9-20, 1999.

[13] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. p. 104-113. Springer-Verlag, 1996.

[14] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. Lecture Notes in Computer Science, 1666 : p. 388-397, 1999.

[15] Michael Tunstall. Smart card security. In Keith Mayes and Konstantinos Markantonakis, editors, Smart Cards, Token, Security and Applications, p. 195-228. Springer, 2008.

[16] Steven Murdoch, Saar Drimer, Ross Anderson, and Mike Bond. Chip and PIN is broken. In David Evans and Giovanni Vigna, editors, SSP 2010, 31st IEEE Symposium on Security & Privacy, Piscataway, NJ, USA, May 2010. IEEE Computer Society Technical Committee on Security and Privacy/The International Association for Cryptologic Research, IEEE Computer Society.

[17] Benot Vibert, Vincent Alimi, and Sylvain Vernois, Analyse de la scurit de transactions puce avec le framework WinSCard Tools, SARSSI 2012.

[18] Mohamad El-Abed, Romain Giot, Baptiste Hemery, and Christophe Rosenberger. A study of users’ acceptance and satisfaction of biometric systems. International Carnahan Conference on Security Technology (ICCST), IEEE, p. 170-178, 2010

[19] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross. Biometrics : A grand challenge. International Conference on Pattern Recognition (ICPR), vol. 2 : p. 935-942,2004.

[20] E. P. Kukula and R. W. Proctor. Human-biometric sensor interaction : Impact of training on biometric system and user performance. In Proceedings of the Symposium on Human Interface 2009 on Human Interface and the Management of Information. Information and Interaction. Part II, vol. 5618, p. 168-177, 2009.

[21] E. P. Kukula, C. R. Blomeke, S. K.Modi, and S. J. Elliott. Effect of human-biometric sensor interaction on fingerprint matching performance, image quality and minutiae count. International Journal of Computer Applications in Technology, 34(4) : p. 270-277, 2009.

[22] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, A.K. Jain, FVC2002: Second Fingerprint Verification Competition International Conference on Pattern Recognition (ICPR), vol. 3, p. 811-814, 2002.

[23] D. Maio, D. Maltoni, J.L. Wayman, A.K. Jain, FVC2004: Third Fingerprint Verification Competition in Proceedings of the First International Conference on Biometric Authentication, 2004

[24] J. Lancia, Un framework de fuzzing pour cartes puce : application aux protocoles emv. SSTIC, 2011.

[25] ISO/IEC 7816-1 to 15 : Identification cards - Integrated circuit(s) cards with contacts (Parts 1 to 15), http://www.iso.org.

[26] M. Martinez-Diaz, J. Fierrez-Aguilar , F. Alonso-Fernandez, et al. Hill-climbing and brute-force attacks on biometric systems: A case study in match-on-card fingerprint verification. In : Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International. IEEE, 2006. p. 151-159.