

# Evaluation of Presentation Attack Detection under the Context of Common Criteria

By

Inés Goicoechea Tellería

A dissertation submitted in partial fulfillment of the requirements for  
the degree of Doctor of Philosophy in

Electrical Engineering, Electronics and Automation

Universidad Carlos III de Madrid

Advisor(s):

Raúl Sánchez Reíllo

Judith Liu Jiménez

Tutor:

Raúl Sánchez Reíllo

June, 2019

Esta tesis se distribuye bajo licencia “Creative Commons **Reconocimiento – No Comercial – Sin Obra Derivada**”



---

# Acknowledgments

---

This section is written in Spanglish, depending on who I am referring to. My apologies for the parts you cannot understand.

Aunque estos 3 años de periodo de gestación hayan sido míos, tengo muchas personas a las que agradecer el acompañamiento y la ayuda. Se me da mal escribir cosas serias y toda la Tesis es seria, así que aquí voy a hacer un poco el tonto.

Lo primerísimo: gracias a mis padres. Al **aitá**, por haberle tenido de ejemplo, que siempre se ha levantado a las 5 de la mañana a leer *papers* (yo no, claro). A la **amá**, por leerse todos mis *papers* e intentar resumírmelos para ver si eran aptos para niños de 5 años, y por tener un gusto hortera al formatear tesis.

Tengo un grupo de amigos peculiar: **Amigos de Guiomar**. Una de las tonterías que hemos hecho ha sido una competición: a ver quién acertaba cuántos *pomodoros* tardaría en redactar la tesis. El que más se acercase, aparecería en las dedicatorias. Redacté la tesis en 145 *pomodoros*. Por lo tanto, el que más confió en mí, el ganador, fue Bubango. El amigo que menos confía en mis habilidades es Néstor. Se queda sin caña de celebración.

Potential winner	Bet	Difference
Bubango	260	115
Vicky	320	175
Arturo	350	205
Juan	450	305
Rubén	451	306
Almudena	500	355
Irene	600	455
Dani	720	575
Rita	740	595
Alba	1000	855
Korn	1200	1055
Nestor	1500	1355

Figura 1: Nivel de confianza de mis amigos en mí.

Gracias a **guitos** y **exguitos**. Historia de Ture: os ronca el mango. Sin vosotros no habría sabido que la Tierra es plana, cómo bloquear una puerta con folios para que no se abra sola, las diferencias entre “ahorita” y “ahora” dependiendo del país, que las patatas no congelan bien, cómo hacer la declaración de la renta, eficiencias energéticas de la calefacción, las ventajas y desventajas del comunismo... Que Dios os lo pague con cinco hijos varones.

Gracias a **Ana** por hacer un TFG espectacular. Sin ti, esta Tesis no sería la mitad de guay. Gracias a todas las personas que se han dejado robar huellas sin tener que apuntarles con una pistola (aunque sería un caso más real y los *papers* habrían quedado mejor, jo).

Thank you, **Kiyoshi Kiyokawa**, for hosting me in Care Lab and for, pun intended, taking care of me and my research. You were always ready to help and give advice and made my stay very smooth. This also includes all the members of Care Lab (and thank you for all the snacks!).

Thank you, “**Amazing People**” group. Notice the quotes. Notice them! We lived in the middle of nowhere in Japan, but you made it feel like home. All those trips around Japan, trips to Aeon and Sushiro and Spanish-like lunches of 4 hours at the Shokudo made my Thesis so much better. Those 8 months will always stay in my little heart <3

Gracias de antebrazo, **Ramón**, por dar siempre el toque de ~~ca~~broneete realismo y por haberme amenizado los múltiples gutiviajes (jo, qué rico el sushi de Sídney). Gracias, **Judith**, por equilibrar todas nuestras inestabilidades emocionales durante la Tesis y por tantas correcciones de *papers* (aunque, admítelo, querías usar el *pencil* del iPad nuevo). Y, sobre todo, gracias a **Raúl**, por darme un montón de oportunidades y confiar en mis habilidades (las de salir de fiesta, digo).

---

# Published and submitted content

---

## Journal papers:

- Goicoechea-Telleria, R. Sanchez-Reillo, J. Liu-Jimenez, and R. Blanco-Gonzalo, “Attack Potential Evaluation in Desktop and Smartphone Fingerprint Sensors: Can They Be Attacked by Anyone?,” *Hindawi*, vol. 2018, pp. 1–13, 2018.
  - Published.
  - Role: performing all the evaluations and writing the paper.
  - Wholly included in Thesis. Chapter 5, Chapter 6, Chapter 7.
  - The inclusion in the thesis of material from this source is specified in a footnote to each chapter where an inclusion occurs.
  - The material from this source included in this thesis is not singled out with typographic means and references
  - URL: <https://www.hindawi.com/journals/wcmc/2018/5609195/>
- Goicoechea-Telleria, K. Kiyokawa, J. L. Jimenez, and R. Sanchez-Reillo, “Low-cost and efficient hardware solution for presentation attack detection in fingerprint biometrics using special lighting microscopes,” *IEEE Access*, vol. 7, pp. 1–1, 2019.
  - Published.
  - Role: performing the evaluation, developing the classification solution and writing the paper.
  - Wholly included in Thesis. Chapter 8.
  - The inclusion in the thesis of material from this source is specified in a footnote to each chapter where an inclusion occurs.
  - The material from this source included in this thesis is not singled out with typographic means and references
  - URL: <https://ieeexplore.ieee.org/document/8600325/>

## Conference papers:

- I. Goicoechea-Telleria, B. Fernandez-Saavedra, and R. Sanchez-Reillo, “An Evaluation of Presentation Attack Detection of Fingerprint Biometric Systems applying ISO / IEC 30107-3,” in *International Biometric Performance Testing Conference*, 2016.
  - Published.
  - Role: performing the evaluation and writing the paper.
  - Wholly included in Thesis. Chapter 5.
  - The inclusion in the thesis of material from this source is specified in a footnote to each chapter where an inclusion occurs.
  - The material from this source included in this thesis is not singled out with typographic means and references

- URL: [http://biometrics.nist.gov/cs\\_links/ibpc2016/presentations/ibpc2016\\_may04/09\\_2016\\_IBPC\\_Goicoechea-Telleria\\_Ines.pdf](http://biometrics.nist.gov/cs_links/ibpc2016/presentations/ibpc2016_may04/09_2016_IBPC_Goicoechea-Telleria_Ines.pdf)
- I. Goicoechea-Telleria, J. Liu-Jimenez, R. Sanchez-Reillo, and W. Ponce-Hernandez, “Vulnerabilities of Biometric Systems integrated in Mobile Devices : an evaluation,” *IEEE Int. Carnahan Conf. Secur. Technol.*, 2016.
  - Published.
  - Role: performing the evaluation and writing the paper.
  - Wholly included in Thesis. Chapter 6, Chapter 7.
  - The inclusion in the thesis of material from this source is specified in a footnote to each chapter where an inclusion occurs.
  - The material from this source included in this thesis is not singled out with typographic means and references
  - URL: <https://ieeexplore.ieee.org/document/7815677/>
- I. Goicoechea-Telleria, A. Garcia-peral, A. Husseis, and R. Sanchez-reillo, “Presentation Attack Detection Evaluation on Mobile Devices : Simplest Approach for Capturing and Lifting a Latent Fingerprint,” in *International Carnahan Conference on Security Technology (ICCST)*, 2018.
  - Published.
  - Role: adapting the evaluation to the ISO standards and writing the paper.
  - Wholly included in Thesis. Chapter 6, Chapter 7.
  - The inclusion in the thesis of material from this source is specified in a footnote to each chapter where an inclusion occurs.
  - The material from this source included in this thesis is not singled out with typographic means and references
  - URL: <https://ieeexplore.ieee.org/document/8585605>
- I. Goicoechea-Telleria, J. Liu-Jimenez, H. Quiros-Sandoval, and R. Sanchez-Reillo, “Analysis of the attack potential in low cost spoofing of fingerprints,” *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2017–Octob, pp. 1–6, 2017.
  - Published.
  - Role: performing the evaluation and writing the paper.
  - Wholly included in Thesis. Chapter 7.
  - The inclusion in the thesis of material from this source is specified in a footnote to each chapter where an inclusion occurs.
  - The material from this source included in this thesis is not singled out with typographic means and references
  - URL: <https://ieeexplore.ieee.org/document/8167798>
- R. B. Gonzalo, B. Corsetti, A. Husseis, and I. Goicoechea-Telleria, “Attacking a smartphone biometric fingerprint system : a novice’s approach,” *2018 Int. Carnahan Conf. Secur. Technol.*, vol. 675087, no. October, pp. 1–5, 2018.
  - Published.
  - Role: creating the tools for performing the evaluation.
  - Wholly included in Thesis. Chapter 7.

- 
- The inclusion in the thesis of material from this source is specified in a footnote to each chapter where an inclusion occurs.
  - The material from this source included in this thesis is not singled out with typographic means and references
  - URL: <https://ieeexplore.ieee.org/document/8585726>

## Other research merits

---

### Journal papers:

- R. Sanchez-Reillo, H. C. Quiros-Sandoval, I. Goicoechea-Telleria, and W. Ponce-Hernandez, “Improving Presentation Attack Detection in Dynamic Handwritten Signature Biometrics,” *IEEE Access*, vol. 5, pp. 20463–20469, 2017.
- R. Blanco-Gonzalo, R. Sanchez-Reillo, I. Goicoechea-Telleria, and B. Strobl, “The mobile pass project: A user interaction evaluation,” *IEEE Trans. Human-Machine Syst.*, vol. 48, no. 3, pp. 311–315, 2018.

### Conference papers:

- R. Sanchez-Reillo, H. Quiros-Sandoval, J. Liu-Jimenez, and I. Goicoechea-Telleria, “Evaluation of strengths and weaknesses of dynamic handwritten signature recognition against forgeries,” *IEEE Int. Carnahan Conf. Secur. Technol.*, pp. 373–378, 2015.
- J. Sanchez-Casanova, I. Goicoechea-Telleria, J. Liu-Jimenez, and R. Sanchez-Reillo, “Performing a Presentation Attack Detection on Voice Biometrics,” *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2018–Octob, pp. 1–5, 2018.

### Standardization contributions to:

- ISO/IEC JTC1/SC37 - Biometric Identification
  - 30107-3: Information technology — Biometric presentation attack detection: Testing and reporting
  - 30107-4: Information technology — Biometric presentation attack detection: Profile for evaluation of mobile devices
  - 21472: Evaluation methodology for user interaction influence in biometric system performance



---

# Abstract

---

THE USE OF Biometrics keeps growing. Every day, we use biometric recognition to unlock our phones or to have access to places such as the gym or the office, so we rely on what security manufacturers offer when protecting our privileges and private life. Moreover, an error in a biometric system can mean that a person can have access to an unintended property, critical infrastructure or cross a border. Thus, there is a growing interest on ensuring that biometric systems work correctly on two fronts: our personal information (smartphones, personal computers) and national security (borders, critical infrastructures).

Given that nowadays we store increasing sensitive data on our mobile devices (documents, photos, bank accounts, etc.), it is crucial to know how secure the protection of the phone really is. Most new smartphones include an embedded fingerprint sensor due to its improved comfort, speed and, as manufacturers claim, security. In the last decades, many studies and tests have shown that it is possible to steal a person's fingerprint and reproduce it, with the intention of impersonating them. This has become a bigger problem as the adoption of fingerprint sensor cell phones have become mainstream.

For the case of border control and critical infrastructures, biometric recognition eases the task of person identification and black-list checking. Although the performance rates for verification and identification have dropped in the last decades, protection against vulnerabilities is still under heavy development. There have been cases in the past where fake fingers have been used to surpass the security of such entities.

The first necessary step for overcoming these issues is to have a common ground for performing security evaluations. This way, different systems' abilities to detect and reject fake fingerprints can be measured and compared against each other. This is achieved by standardization and the corresponding certification of biometric systems. The new software and hardware presentation attack detection techniques shall undergo tests that follow such standards.

The aim of this Thesis is two-fold: evaluating commercial fingerprint biometric systems against presentation attacks (fake fingers) and developing a new presentation attack detection method for overcoming these attacks. Moreover, through this process, several contributions were proposed and accepted in international ISO standards.

On the first matter, a few questions are meant to be answered: it is well known that it is possible to hack a smartphone using fake fingers made of Play-Doh and other easy-to-obtain materials but, to what extent? Is this true for all users or only for specialists with deep knowledge on Biometrics? Does it matter who the person doing the attack is, or are all attackers the same when they have the same base knowledge? Are smartphone fingerprint sensors as reliable as desktop sensors? What is the easiest way of stealing a fingerprint from someone? To answer these, five experiments were

performed on several desktop and smartphone fingerprint readers, including many different attackers and fingerprint readers. As a general result, all smartphone capture devices could be successfully hacked by inexperienced people with no background in Biometrics. All of the evaluations followed the pertinent standards, ISO/IEC 30107 Parts 3 and 4 and Common Criteria and an analysis of the attack potential was carried out. Moreover, the knowledge gathered during this process served to make methodological contributions to the above-mentioned standards.

Once some expertise had been gathered on attacking fingerprint sensors, it was decided to develop a new method to detect fake fingerprints. The aim was to find a low-cost and efficient system to solve this issue. As a result, a new optical system was used to capture fingerprints and classify them into real or fake samples. The system was tested by performing an evaluation using 5 different fake finger materials, obtaining much lower error rates than those reported in the state of the art at the moment this Thesis was written.

The contributions of this Thesis include:

- Improvements on the presentation attack detection evaluation methodology.
- Contributions to ISO/IEC 30107 - Biometric presentation attack detection - Part 3: *Testing and reporting* and Part 4: *Profile for evaluation of mobile devices*.
- Presentation attack detection evaluations on commercial desktop and smartphone fingerprint sensors following ISO/IEC 30107-3 and 4.
- A new low-cost and efficient optical presentation attack detection mechanism and an evaluation on the said system.

---

# Resumen

---

EL USO DE la Biometría está en constante crecimiento. Cada día, utilizamos reconocimiento biométrico para desbloquear nuestros teléfonos o para tener acceso a lugares como el gimnasio o la oficina, por lo que confiamos en lo que los fabricantes ofrecen para proteger nuestros privilegios y nuestra vida privada. Además, un error en un sistema biométrico puede significar que una persona pueda tener acceso a una propiedad no debida, a una infraestructura crítica o a cruzar una frontera. Por lo tanto, existe un interés creciente en asegurar que los sistemas biométricos funcionen correctamente en dos frentes: nuestra información personal (teléfonos inteligentes, ordenadores personales) y la seguridad nacional (fronteras, infraestructuras críticas).

Dado que hoy en día almacenamos cada vez más datos sensibles en nuestros dispositivos móviles (documentos, fotos, cuentas bancarias, etc.), es crucial saber cómo de segura es realmente la protección del teléfono. La mayoría de los nuevos teléfonos inteligentes incluyen un sensor de huellas dactilares integrado debido a su mayor comodidad, velocidad y, como afirman los fabricantes, seguridad. En las últimas décadas, muchos estudios y pruebas han demostrado que es posible robar la huella dactilar de una persona y reproducirla, con la intención de hacerse pasar por ella. Esto se ha convertido en un problema mayor a medida que la adopción de los teléfonos celulares con sensor de huellas dactilares se ha ido generalizando.

En el caso del control fronterizo y de las infraestructuras críticas, el reconocimiento biométrico facilita la tarea de identificación de las personas y la comprobación de listas negras. Aunque las tasas de rendimiento en materia de verificación e identificación han disminuido en las últimas décadas, la protección antifraude todavía está bajo intenso desarrollo. Existen casos en los que se han utilizado dedos falsos para vulnerar la seguridad de dichas entidades.

El primer paso necesario para superar estos problemas es contar con una base común desde la que realizar evaluaciones de seguridad. De esta manera, se pueden medir y comparar las capacidades de los diferentes sistemas para detectar y rechazar huellas dactilares falsas. Esto se consigue mediante la estandarización y la correspondiente certificación de los sistemas biométricos. Las nuevas técnicas de detección de ataques de presentación de software y hardware deben someterse a pruebas que se ajusten a dichas normas.

Esta Tesis tiene dos objetivos: evaluar los sistemas biométricos de huellas dactilares comerciales contra ataques de presentación (dedos falsos) y desarrollar un nuevo método de detección de ataques de presentación para disminuir la eficacia de estos ataques. Además, a través de este proceso, se propusieron y aceptaron varias contribuciones en las normas internacionales ISO.

Sobre el primer asunto, hay que responder algunas preguntas: es bien sabido que es posible *hackear* un teléfono inteligente con dedos falsos hechos de Play-Doh y otros materiales fáciles de obtener, pero ¿hasta qué punto? ¿Es esto cierto para todos los

usuarios o sólo para los especialistas con un profundo conocimiento de la Biometría? ¿Importa quién es la persona que realiza el ataque, o todos los atacantes son iguales cuando parte de la misma base de conocimiento? ¿Son los sensores de huellas dactilares de los teléfonos inteligentes tan fiables como los de sobremesa? ¿Cuál es la manera más fácil de robar una huella digital a alguien? Para responder estas preguntas, se realizaron cinco experimentos en varios lectores de huellas dactilares de escritorio y de teléfonos inteligentes, incluyendo muchos atacantes y lectores de huellas dactilares diferentes. Como resultado general, todos los dispositivos de captura pudieron ser *hackeados* con éxito por personas sin experiencia en Biometría. Todas las evaluaciones siguieron las normas pertinentes, ISO/IEC 30107 Partes 3 y 4 y Common Criteria y se llevó a cabo un análisis del potencial de ataque. Además, los conocimientos adquiridos durante este proceso sirvieron para aportar una contribución metodológica a las normas mencionadas.

Una vez adquiridos algunos conocimientos sobre ataques a sensores de huellas dactilares, se decidió desarrollar un nuevo método para detectar huellas falsas. El objetivo era encontrar un sistema de bajo coste y eficiente para resolver este problema. Como resultado, se utilizó un nuevo sistema óptico para capturar las huellas dactilares y clasificarlas en muestras reales o falsas. El sistema se probó mediante la realización de una evaluación utilizando 5 materiales de dedos falsos diferentes, obteniendo tasas de error mucho más bajas que las reportadas en el estado del arte en el momento de redactar esta Tesis.

Las contribuciones de esta Tesis incluyen:

- Mejoras en la metodología de evaluación de detección de ataques de presentación.
- Contribuciones a “ISO/IEC 30107 - Biometric presentation attack detection - Part 3: *Testing and reporting*” y “Part 4: *Profile for evaluation of mobile devices*”.
- Evaluaciones de detección de ataques de presentación en sensores de huellas dactilares comerciales de escritorio y de teléfonos inteligentes siguiendo la norma ISO/IEC 30107-3 y 4.
- Un nuevo y eficiente mecanismo óptico de detección de ataques de presentación, de bajo coste, y una evaluación de dicho sistema.

---



---

# Table of contents

ACKNOWLEDGMENTS	I
ABSTRACT	VII
RESUMEN	IX
TABLE OF CONTENTS	XIII
LIST OF FIGURES	XV
LIST OF TABLES	XVII
LIST OF ACRONYMS	XIX
LIST OF SYMBOLS	XX
<b>CHAPTER 1. INTRODUCTION</b>	<b>1</b>
<b>CHAPTER 2. BIOMETRIC RECOGNITION</b>	<b>7</b>
2.1 <i>A brief history of biometric recognition</i>	7
2.2 <i>Biometric recognition systems</i>	9
2.3 <i>Security evaluation of fingerprint biometric systems</i>	10
<b>CHAPTER 3. STATE OF THE ART</b>	<b>15</b>
3.1 <i>Fingerprint sensors</i>	15
3.2 <i>Presentation attack detection evaluation</i>	17
3.3 <i>Presentation attack detection mechanisms</i>	19
<b>CHAPTER 4. PRESENTATION ATTACK DETECTION EVALUATION METHODOLOGY AND STUDIES</b>	<b>23</b>
4.1 <i>Planning the evaluation</i>	25
4.2 <i>Execution of the evaluation</i>	28
4.3 <i>Results reporting</i>	29
4.4 <i>PAD evaluation studies overview</i>	30
<b>CHAPTER 5. PRESENTATION ATTACK DETECTION EVALUATION OF DESKTOP FINGERPRINT SENSORS</b>	<b>33</b>
5.1 <i>Planning</i>	34
5.2 <i>Execution</i>	40
5.3 <i>Results</i>	40
5.4 <i>Conclusions</i>	50
5.5 <i>Contributions and dissemination</i>	51
<b>CHAPTER 6. PRESENTATION ATTACK DETECTION EVALUATION OF MOBILE DEVICES - SINGLE EXPERTS</b>	<b>53</b>
6.1 <i>Planning</i>	55
6.2 <i>Execution</i>	61
6.3 <i>Results</i>	62
6.4 <i>Conclusions</i>	67
6.5 <i>Contributions and dissemination</i>	68
<b>CHAPTER 7. PRESENTATION ATTACK DETECTION EVALUATION ON MOBILE DEVICES - MULTIPLE NON-EXPERTS</b>	<b>69</b>
7.1 <i>Planning</i>	72
7.2 <i>Results</i>	76
7.3 <i>Comparison with expert attackers</i>	85
7.4 <i>Conclusions</i>	91
7.5 <i>Contributions and dissemination</i>	91
<b>CHAPTER 8. DETECTION OF PRESENTATION ATTACKS</b>	<b>93</b>
8.1 <i>Narrow-band camera</i>	94
8.2 <i>Microscopes with special lighting</i>	100

<b>CHAPTER 9. CONCLUSIONS AND FUTURE WORK</b>	<b>113</b>
9.1 <i>Conclusions</i>	113
9.2 <i>Future work</i>	115
REFERENCES	117



# List of Figures

FIGURE 1. REASONING AND UNIFYING THREAD OF EACH STUDY. ....	2
FIGURE 2. THESIS STRUCTURE OUTLINE. ....	4
FIGURE 3. COMPONENTS OF A BIOMETRIC SYSTEM [33]. ....	9
FIGURE 4. DIAGRAM OF THE FOCUS OF THIS THESIS. ....	10
FIGURE 5. VULNERABILITY POINTS IN A BIOMETRIC RECOGNITION SYSTEM [33]. ....	11
FIGURE 6. DIAGRAM OF CATEGORIES OF THE IUT (ITEM UNDER TEST). ....	13
FIGURE 7. CAPACITIVE FINGERPRINT SENSOR [34] ....	16
FIGURE 8. OPTICAL FINGERPRINT SENSOR [34] ....	16
FIGURE 9. THERMAL FINGERPRINT SENSOR [34] ....	16
FIGURE 10. NEW METHODOLOGY DEVELOPED FOR TESTING PAD IN MOBILE DEVICES. ....	24
FIGURE 11. STEPS NEEDED FOR BIOMETRIC EVALUATIONS. ....	25
FIGURE 12. METRICS USED FOR EACH CASE. DESKTOP FINGERPRINT SENSORS GIVE US MORE INTERMEDIATE DECISIONS THAN MOBILE DEVICES. ....	29
FIGURE 13. OVERVIEW OF ALL CARRIED OUT PAD EVALUATION STUDIES. ....	31
FIGURE 14. OVERVIEW OF STUDY 1 CHARACTERISTICS. ....	34
FIGURE 15. PROCESS FOR OBTAINING MOLDS: A) COOPERATIVE SILICON MOLD AFTER HAVING A PRESSED FINGER, B) FINGERPRINTS PRINTED ON TRANSPARENT SHEET, C) PCB BOARD BEING DEVELOPED AND D) RESULTING NON-COOPERATIVE PCB MOLD. ....	36
FIGURE 16. RESULTING ARTEFACTS: E) PLAY-DOH ARTEFACT, F) GELATIN ARTEFACT ON A NON-COOPERATIVE MOLD, G) LATEX WITH GRAPHITE ARTEFACT AND H) LATEX ARTEFACT ON A COOPERATIVE MOLD DURING THE DRYING PROCESS. ....	36
FIGURE 17. EXAMPLE DISPLAY OF THE DESKTOP CAPTURE PROGRAM. ....	39
FIGURE 18. RESULTS REPORTING METRICS, ACCORDING TO ISO/IEC 30107-3. THIS APPLIES TO ALL SENSORS. ....	41
FIGURE 19. IAPMR, IAPNMR, 1-APAR AND APNRR FOR EACH PAI SPECIES AND EACH DEVICE, FOR THE CASE OF COOPERATIVE ATTACKS. ....	45
FIGURE 20. IAPMR, IAPNMR, 1-APAR AND APNRR FOR EACH PAI SPECIES AND EACH DEVICE, FOR THE CASE OF NON-COOPERATIVE ATTACKS. ....	49
FIGURE 21. REASONING FOR EVALUATIONS ON MOBILE DEVICES PERFORMED BY SINGLE EXPERT ATTACKERS. ....	53
FIGURE 22. OVERVIEW OF EVALUATIONS ON MOBILE DEVICES PERFORMED BY EXPERT ATTACKERS. THE SYMBOL LEGEND CAN BE FOUND ON THE LIST OF SYMBOLS. ....	54
FIGURE 23. LATENT FINGERPRINTS LEFT ON THE SURFACE BY TAPPING THE GENUINE USER'S FINGER. ....	57
FIGURE 24. PICTURE WITH FLASH BEING TAKEN WITH THE ATTACKER'S CAMERA. ....	57
FIGURE 25. (A) PICTURE TAKEN WITH SCANNER APP WITH FLASH, WHERE FINGERPRINT IS ALREADY VISIBLE. (B) FINGERPRINT ZOOMED IN. (C) BACKGROUND ERASED WITH IMAGE EDITING PROGRAM, RESULT ON (D). (E) THRESHOLD ADJUSTMENT AND (F) FINAL RESULT. ....	58
FIGURE 26. (A) FINGERPRINT IMAGE PRINTED ON A TRANSPARENT SHEET (B) PBC BOARD BEING DEVELOPED (C) RESULT AFTER ETCHING PCB BOARD MOLD (D) PLAY-DOH ARTEFACT ON THE PCB MOLD. ....	58
FIGURE 27. SMARTPHONE APP (ANDROID AND IOS) FOR LOGGING THE PAD EVALUATION. A PASS/FAIL RESULT IS LOGGED FOR EACH ATTEMPT. ....	59
FIGURE 28. IAPMR AND IAPNMR METRICS, ACCORDING TO ISO/IEC 30107-3. ....	62
FIGURE 29. IAPMR PER DEVICE, STUDIES 2 AND 3 TOGETHER. ....	63
FIGURE 30. NUMBER OF SUCCESSFUL (IN RED) AND FAILED (IN GREEN) ATTACKS FOR EACH MOBILE DEVICE. STUDIES 2 AND 3 TOGETHER. ....	63
FIGURE 31. IAPMR PER DEVICE (MD1-MD5) AND PER STUDY (2-3). <i>C</i> = COOPERATIVE ATTACKS (STUDY 2) AND <i>NC</i> = NON-COOPERATIVE ATTACKS (STUDY 3). ....	64
FIGURE 32. NUMBER OF SUCCESSFUL (IN RED) AND FAILED (IN GREEN) ATTACKS FOR EACH MOBILE DEVICE, DIVIDED BY STUDY AND COOPERATION TYPE. ....	65
FIGURE 33. IAPMR PER DEVICE, PER STUDY AND PER PAI SPECIES. <i>C</i> = COOPERATIVE ATTACKS (STUDY 2) AND <i>NC</i> = NON-COOPERATIVE ATTACKS (STUDY 3). <i>P</i> = PLAY-DOH, <i>G</i> = GELATIN, <i>L</i> = LATEX WITH GRAPHITE AND <i>W</i> = WHITE GLUE WITH GRAPHITE. ....	65
FIGURE 34. NUMBER OF SUCCESSFUL (RED) AND FAILED (GREEN) ATTACKS BY STUDY, DEVICE AND PAI SPECIES. <i>C</i> = COOPERATIVE ATTACKS (STUDY 2) AND <i>NC</i> = NON-COOPERATIVE ATTACKS (STUDY 3). <i>P</i> = PLAY-DOH, <i>G</i> = GELATIN, <i>L</i> = LATEX WITH GRAPHITE AND <i>W</i> = WHITE GLUE WITH GRAPHITE. ....	66
FIGURE 35. REASONING FOR EVALUATIONS ON MOBILE DEVICES PERFORMED BY MULTIPLE NON-EXPERT ATTACKERS. ....	69

FIGURE 36. OVERVIEW OF EVALUATIONS ON MOBILE DEVICES PERFORMED BY MULTIPLE NON-EXPERT ATTACKERS. .... 71

FIGURE 37. IAPMR AND IAPNMR METRICS, ACCORDING TO ISO/IEC 30107-3.....76

FIGURE 38. IAPMR PER DEVICE, BOTH EXPERIMENTS TOGETHER. ....77

FIGURE 39. NUMBER OF SUCCESSFUL (IN RED) AND FAILED (IN GREEN) ATTACKS FOR EACH MOBILE DEVICE. BOTH EXPERIMENTS TOGETHER. ....77

FIGURE 40. IAPMR PER DEVICE (MD1-MD6) AND PER STUDY (4-5). .... 78

FIGURE 41. NUMBER OF SUCCESSFUL (IN RED) AND FAILED (IN GREEN) ATTACKS FOR EACH MOBILE DEVICE, DIVIDED BY STUDY. .... 78

FIGURE 42. IAPMR RESULTS PER MOBILE DEVICE, STUDY AND ATTACKER. .... 80

FIGURE 43. NUMBER OF SUCCESSFUL (IN RED) AND FAILED (IN GREEN) ATTACKS FOR EACH MOBILE DEVICE, DIVIDED BY STUDY AND BY ATTACKER.....81

FIGURE 44. IAPMR FOR EACH PAI SPECIES, DIVIDED BY MOBILE DEVICE (MD1-MD6). THE THREE MOST SUCCESSFUL PAI SPECIES ARE MARKED IN A DIFFERENT COLOR. .... 82

FIGURE 45. NUMBER OF SUCCESSFUL (IN RED) AND FAILED (IN GREEN) ATTACKS, DIVIDED BY DEVICE AND PAI SPECIES. .... 84

FIGURE 46. CHARACTERISTICS OF STUDIES. .... 86

FIGURE 47. IAPMR RESULTS DIVIDED BY MOBILE DEVICE AND STUDY. THE COLORS CORRESPOND TO EXPERT/NON-EXPERT ATTACKERS. .... 86

FIGURE 48. PASS AND FAIL RESULTS DIVIDED BY MOBILE DEVICE AND STUDY..... 87

FIGURE 49. IAPMR FOR EACH ATTACKER, DIVIDED BY STUDY AND DEVICE. .... 89

FIGURE 50. PASSES AND FAILS FOR EACH ATTACKER, DIVIDED BY STUDY AND MOBILE DEVICE. .... 90

FIGURE 51. SETUP OF THE NARROW-BAND CAMERA AND BONA FIDE SUBJECT HOLDING FINGER READY FOR CAPTURE..... 94

FIGURE 52. EXAMPLES OF REAL AND ARTEFACT SAMPLES AT 550NM AND 630NM. .... 96

FIGURE 53. BAG OF FEATURES OR BAG OF VISUAL WORDS DIAGRAM. ....97

FIGURE 54. APCER AND BPCER FOR EACH WAVELENGTH. THE THREE LOWEST RESULTS FOR APCER AND BPCER ARE MARKED IN YELLOW..... 98

FIGURE 55. DIFFERENT SKIN PENETRATION LEVELS DEPENDING ON WAVELENGTH OF DIGITAL MICROSCOPES. .... 101

FIGURE 56. EXAMPLES OF REAL AND PAI IMAGES CAPTURED IN DIFFERENT WAVELENGTHS. ....103

FIGURE 57. EXAMPLES OF NON-CONFORMANT FINGERPRINTS OF ONE USER OF THE DATABASE WITH A SKIN DISEASE, IN DIFFERENT WAVELENGTHS. ....104

FIGURE 58. APCER CROSS-COMPARISON RESULTS FOR EACH LIGHTING MODE. EVERY RESULT WAS CALCULATED 10 TIMES AND THEN AVERAGED.....105

FIGURE 59. BPCER CROSS-COMPARISON RESULTS FOR EACH LIGHTING MODE. EVERY RESULT WAS CALCULATED 10 TIMES AND THEN AVERAGED.....105

FIGURE 60. APCER AND BPCER RESULTS SEPARATED BY WAVELENGTH AND CHANNEL. 70% TRAINING, 30% TESTING.....106

FIGURE 61. NOTICEABLE VARIATION IN R CHANNEL.....106

FIGURE 62. APCER CROSS-COMPARISON WITH DIFFERENT PAI SPECIES. PLA = PLAY-DOH, GLT = GELATIN, NPL = NAIL POLISH, WGL = WHITE GLUE, LTX = LATEX. ....107

FIGURE 63. BPCER CROSS-COMPARISON WITH DIFFERENT PAI SPECIES. PLA = PLAY-DOH, GLT = GELATIN, NPL = NAIL POLISH, WGL = WHITE GLUE, LTX = LATEX. ....107

FIGURE 64. APCER AND BPCER CALCULATED BY PAI SPECIES, WAVELENGTH AND RGB CHANNEL..... 108

FIGURE 65. APCER AND BPCER CALCULATED BY PAI SPECIES, WAVELENGTH AND RGB CHANNEL. APCER + BPCER OUTLIERS GREATER THAN 20% ARE DELETED FOR CLARIFICATION. ....109

FIGURE 66. APCER AND BPCER RESULTS FOR DIFFERENT IMAGE SIZES, AS WELL AS TIME ELAPSED FOR CLASSIFYING 1 IMAGE..... 110

---

# List of Tables

TABLE 1. IAPMR RESULTS AND CHARACTERISTICS OF EACH EVALUATION. ONLY EXPERIMENTS WITH REPORTED NUMERICAL RESULTS ARE SHOWN. ....	18
TABLE 2. SOFTWARE PAD PERFORMANCE WITH INDEPENDENT EVALUATORS. RESULTS WERE GATHERED FROM [47]. ....	19
TABLE 3. SOFTWARE PAD PERFORMANCE WITH SELF-DECLARED RESULTS AND EVALUATIONS. RESULTS WERE GATHERED FROM [47]. ....	20
TABLE 4. HARDWARE PAD PERFORMANCE. ....	21
TABLE 5. CALCULATION OF ATTACK POTENTIAL. EACH CATEGORY IS ASSIGNED A VALUE ACCORDING TO THIS TABLE [18]. ....	27
TABLE 6. RATING OF VULNERABILITIES AND TOE RESISTANCE [18]. ....	27
TABLE 7. IDENTIFICATION OF ALL POSSIBLE THREATS AND ATTACKS: DESCRIPTION OF TOE. ....	35
TABLE 8. IDENTIFICATION OF ALL POSSIBLE THREATS AND ATTACKS: DESCRIPTION OF TARGET APPLICATION. ....	35
TABLE 9. PLANNING: ANALYSIS OF ATTACK POTENTIAL BY SEARCHING THREATS AND THEIR CORRESPONDING ATTACKS (STUDY ON DESKTOP SENSORS). ....	36
TABLE 10. ATTACK POTENTIAL CALCULATION FOR COOPERATIVE ATTACKS ON DESKTOP FINGERPRINT SENSORS. SCORES ASSIGNED ACCORDING TO THE CLASSIFICATION FROM COMMON CRITERIA [18, P. 429]. ....	37
TABLE 11. ATTACK POTENTIAL CALCULATION FOR NON-COOPERATIVE ATTACKS ON DESKTOP FINGERPRINT SENSORS. SCORES ASSIGNED ACCORDING TO THE CLASSIFICATION FROM COMMON CRITERIA [18, P. 429]. ....	38
TABLE 12. PENETRATION TEST CHARACTERISTICS FOR THE STUDY ON DESKTOP SENSORS. ....	39
TABLE 13. NFIQ DISTRIBUTION BY SENSOR FOR COOPERATIVE ATTACKS, FOR THE CASE OF GELATIN. ....	42
TABLE 14. NFIQ DISTRIBUTION BY SENSOR FOR COOPERATIVE ATTACKS, FOR THE CASE OF PLAY-DOH. ....	42
TABLE 15. NFIQ DISTRIBUTION BY SENSOR FOR COOPERATIVE ATTACKS, FOR THE CASE OF LATEX. ....	42
TABLE 16. NFIQ DISTRIBUTION BY SENSOR FOR COOP. ATTACKS, FOR THE CASE OF LATEX+GRAPHITE. ....	43
TABLE 17. NFIQ DISTRIBUTION BY SENSOR FOR COOPERATIVE ATTACKS, FOR THE CASE OF SILICONE. ....	43
TABLE 18. NFIQ DISTRIBUTION BY SENSOR FOR COOPERATIVE ATTACKS, FOR THE CASE OF SILICONE WITH GRAPHITE. ....	43
TABLE 19. NFIQ DISTRIBUTION BY SENSOR FOR COOPERATIVE ATTACKS, FOR THE CASE OF WHITE GLUE. ....	44
TABLE 20. NUMBER OF ARTEFACTS BUILT WITH EACH MATERIAL FOR THE CASE OF COOPERATIVE ATTACKS. ....	45
TABLE 21. NFIQ DISTRIBUTION BY SENSOR FOR NON-COOPERATIVE ATTACKS, FOR THE CASE OF GELATIN. ....	46
TABLE 22. NFIQ DISTRIBUTION BY SENSOR FOR NON-COOP. ATTACKS, FOR THE CASE OF PLAY-DOH. ....	47
TABLE 23. NFIQ DISTRIBUTION BY SENSOR FOR NON-COOPERATIVE ATTACKS, FOR THE CASE OF LATEX. ....	47
TABLE 24. NFIQ DISTRIBUTION DIVIDED BY SENSOR FOR NON-COOP. ATTACKS, FOR LATEX+ GRAPHITE. ....	47
TABLE 25. NFIQ DISTRIBUTION BY SENSOR FOR NON-COOP. ATTACKS, FOR THE CASE OF SILICONE. ....	48
TABLE 26. NFIQ DISTRIBUTION BY SENSOR FOR NON-COOP. ATTACKS, FOR SILICONE WITH GRAPHITE. ....	48
TABLE 27. NFIQ DISTRIBUTION BY SENSOR FOR NON-COOP. ATTACKS, FOR THE CASE OF WHITE GLUE. ....	48
TABLE 28. NUMBER OF ARTEFACTS BUILT WITH EACH MATERIAL FOR THE CASE OF NON-COOPERATIVE ATTACKS. ....	50
TABLE 29. LIST OF VULNERABILITIES OF DESKTOP SENSORS. IT MUST BE NOTED THAT NOT ALL PAI SPECIES WERE TRIED ON EVERY READER AND THAT DIFFERENT NUMBERS OF ATTEMPTS WERE PERFORMED ON EACH EXPERIMENT. ....	50
TABLE 30. IDENTIFICATION OF ALL POSSIBLE THREATS AND ATTACKS: DESCRIPTION OF TOE. ....	55
TABLE 31. IDENTIFICATION OF ALL POSSIBLE THREATS AND ATTACKS: DESCRIPTION OF TARGET APPLICATION. ....	56
TABLE 32. PLANNING: ANALYSIS OF ATTACK POTENTIAL BY SEARCHING THREATS AND THEIR CORRESPONDING ATTACKS (ALL STUDIES ON MOBILE DEVICES). ....	59
TABLE 33. ATTACK POTENTIAL CALCULATION FOR COOPERATIVE ATTACKS ON SMARTPHONE FINGERPRINT SENSORS. ....	60
TABLE 34. ATTACK POTENTIAL CALCULATION FOR NON-COOPERATIVE ATTACKS ON SMARTPHONE FINGERPRINT SENSORS. ....	60
TABLE 35. PENETRATION TEST CHARACTERISTICS FOR THE STUDY ON SMARTPHONE SENSORS PERFORMED BY EXPERT ATTACKERS. ....	61
TABLE 36. LIST OF VULNERABILITIES OF SMARTPHONES. NOT ALL PAI SPECIES WERE TRIED ON EVERY PHONE AND THAT DIFFERENT NUMBERS OF ATTEMPTS WERE PERFORMED ON EACH EXPERIMENT. ....	66
TABLE 37. IDENTIFICATION OF ALL POSSIBLE THREATS AND ATTACKS: DESCRIPTION OF TOE. ....	72
TABLE 38. IDENTIFICATION OF ALL POSSIBLE THREATS AND ATTACKS: DESCRIPTION OF TARGET APPLICATION. ....	73












TABLE 39. PLANNING: ANALYSIS OF ATTACK POTENTIAL BY SEARCHING THREATS AND THEIR CORRESPONDING ATTACKS (ALL STUDIES ON MOBILE DEVICES). .....	74
TABLE 40. ATTACK POTENTIAL CALCULATION FOR COOPERATIVE ATTACKS ON SMARTPHONE FINGERPRINT SENSORS. ....	74
TABLE 41. PENETRATION TEST CHARACTERISTICS FOR THE STUDY ON SMARTPHONE SENSORS PERFORMED BY MULTIPLE NON-EXPERT ATTACKERS. ....	75
TABLE 42. LIST OF VULNERABILITIES OF SMARTPHONES. IT MUST BE NOTED THAT NOT ALL PAI SPECIES WERE TRIED ON EVERY PHONE AND THAT DIFFERENT NUMBERS OF ATTEMPTS WERE PERFORMED ON EACH EXPERIMENT. ....	85
TABLE 43. DETAILS OF THE DATABASE FOLLOWING REQUIREMENTS OF ISO/IEC 30107-3. ....	95
TABLE 44. APCER AND BPCER VALUES FOR EACH WAVELENGTH (INCREMENTS OF 10NM AND RGB). 70% TRAINING, 30% TESTING. ....	98
TABLE 45. CROSS VALIDATION OF APCER AND BPCER RESULTS FOR THE SELECTED WAVELENGTHS STUDY. ALL VALUES WERE CALCULATED 20 TIMES AND THEN AVERAGED. ....	99
TABLE 46. CROSS VALIDATION OF APCER AND BPCER RESULTS FOR THE IMAGE ALIGNMENT AND SUBTRACTION STUDY. ALL VALUES WERE CALCULATED 20 TIMES AND THEN AVERAGED. ....	99
TABLE 47. DETAILS OF THE DATABASE FOLLOWING REQUIREMENTS OF ISO/IEC 30107-3. ....	102
TABLE 48. APCER AND BPCER CROSS-COMPARISON OF 575/610NM WAVELENGTH SAMPLES IN THE RED CHANNEL. ....	107
TABLE 49. LOWEST ERROR RATES FOR EACH PAI SPECIES. LOWER ERROR RATE CONSIDERS THE LOWEST APCER AND BPCER COMBINATION. ....	108
TABLE 50. APCER AND BPCER CROSS-COMPARISON OF 575/610NM WAVELENGTH SAMPLES IN THE RED CHANNEL, LEAVING OUT ONE CAPTURE SUBJECT'S NON-CONFORMANT FINGERPRINTS DUE TO A SKIN DISEASE. RESULTS WERE AVERAGED 10 TIMES. ....	110
TABLE 51. DECREASE OF APCER AND BPCER LEAVING OUT THE CAPTURE SUBJECT WITH A SKIN DISEASE. ...	110

---

# List of Acronyms

ABC	Automatic Border Control
APAR	Attack Presentation Acquisition Rate
APCER	Attack Presentation Classification Error Rate
BPCER	Bona-fide Classification Error Rate
CC	Common Criteria for Information Technology Security Evaluation
CEN	European Committee for Standardization
CEM	Common Methodology for Information Technology Security Evaluation
IAPMR	Impostor Attack Presentation Match Rate
IAPNMR	Impostor Attack Presentation Non-Match Rate
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IUT	Item Under Test
NFIQ	NIST Fingerprint Image Quality
NIST	National Institute of Standards and Technology
PAI	Presentation Attack Instrument
PAD	Presentation Attack Detection
PCB	Printed Circuit Board
TOE	Target of Evaluation

## List of Symbols

-  One attacker
-  Multiple attackers
-  Cooperative attacks
-  Non-cooperative attacks
-  Thermal fingerprint sensor
-  Capacitive fingerprint sensor 1
-  Capacitive fingerprint sensor 2
-  Optical fingerprint sensor
-  Grey box. Access to NFIQ and pass/fail results
-  Black box. Access to pass/fail results
-  Number of fingers for fingerprint sources

---





# Chapter 1. Introduction

---

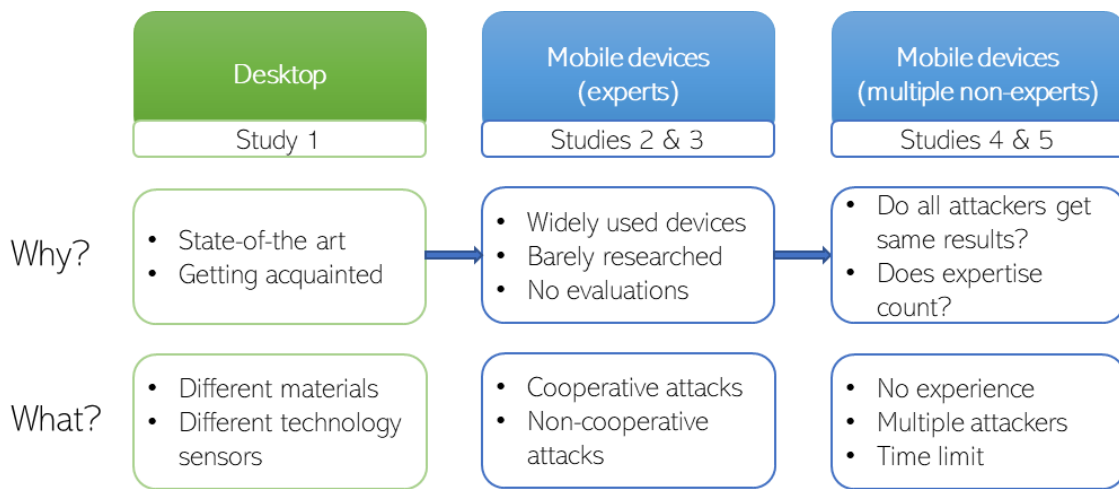
BIOMETRIC RECOGNITION HAS become a commonplace technology in our everyday lives. We use it to unlock our phones, to get in the gym or to enter the office due to its comfort of use [4] and freeing us from remembering passwords [5], [6]. Nevertheless, when sensitive data (personal pictures, documents) or privileges (gym membership, food coupons) are at stake, we need to make sure that we know how secure these systems are.

There have been many tests of fingerprint sensors' ability to detect attacks in the last decade [7]–[15]. For that end, different materials were used to create fake fingers and use them on capture devices, to check if an attacker would be able to bypass the security. When the first smartphones with embedded fingerprint sensors were released, fake fingers were created to try to attack the system, and succeeded [16]. It was rapidly spread on the media that biometric recognition was not secure, and that people should not trust it. Soon after, it was proven that an attacker can steal a person's fingerprint by taking a picture of it from a distance [17].

The simulated attackers that performed these tests were, to the best of our knowledge, researchers or proficient in Biometrics. Moreover, the released videos only show one attempt, which showed to be successful. However: how many attempts did they need until it worked? How long had they been working on Biometrics? What was their expertise? These questions were left unanswered.

To answer them, it is necessary to follow a common methodology to have comparable security evaluations and to give a complete understanding of how the systems behave against attacks. This is what was achieved with this work. To fulfill the need of comparable security evaluations, there are several tools like Common Criteria

[3] and its evaluation methodology, CEM (Common Methodology for Information Technology Security Evaluation) [18]. Although, these are focused on Information Technology security in general and need some adaptation for the case of Biometrics. More particularly, for the attacks at the capture level, the so-called presentation attacks. Hence, a new family of ISO standard was created, ISO/IEC 30107-x [1], to address the need of standardizing the evaluation of Presentation Attack Detection (PAD). Also, some other works have been done covering methodologies and best practices to evaluate security [19][20] and to evaluate the performance of sensors embedded in smartphones [21]. A methodology unifying both was proposed in [22]. This work gathers 5 studies following thoroughly these standards, in order to give a complete answer to the attack resistance ability of these systems. The reasons that motivated the studies and what was done in each are detailed on Figure 1. The thesis structure is outlined on Figure 2.



**Figure 1. Reasoning and unifying thread of each study.**

First, the idea was to get acquainted with the state of the art in fingerprint sensor attacks by trying different fake fingers on 4 desktop readers: 1 thermal, 2 capacitive and 1 optical. In total, 4,672 attacks were attempted using 7 different PAI species (fake finger material) [23]. Both cooperative and non-cooperative tests were made (that is, with and without collaboration from the capture subject). Also, the results were reported according to one of the very first drafts of the more recently published ISO/IEC standard (i.e. ISO/IEC 30107 - *Biometric presentation attack detection*).

Once expertise had been gained on this first approach to fingerprint attacks, it was decided to aim for the case of mobile devices for three main reasons: they are widely and increasingly used devices, it has barely been researched and no evaluations have been performed, at least publicly. To gain a wide overview of the matter, 4 different studies were carried out on attacks on mobile devices (studies 2-5).

For study 2, the 3 most interesting PAI species (according to ease of production, success on attacks or level of resemblance to real finger) from the first study were chosen to attempt attacks on 5 smartphones that have embedded fingerprint sensors, summing a total of 2,669 attacks [22]. This experiment was performed by the same evaluator of the first experiment (the author of this Thesis), thus having gathered

knowledge on how to perform attacks. All the artefacts were created in a collaborative manner in this case.

For the third study, the goal was to find the easiest way to steal a latent fingerprint from someone's phone screen. This way, it would emulate the case of an attacker stealing a smartphone and then using the fingerprints from the screen to create artefacts and attack the capture device. Thus, in this case, the attacks were non-cooperative. In total, 17,100 attack attempts were performed on the same 5 smartphones from the previous evaluation, and all smartphones were successfully attacked.

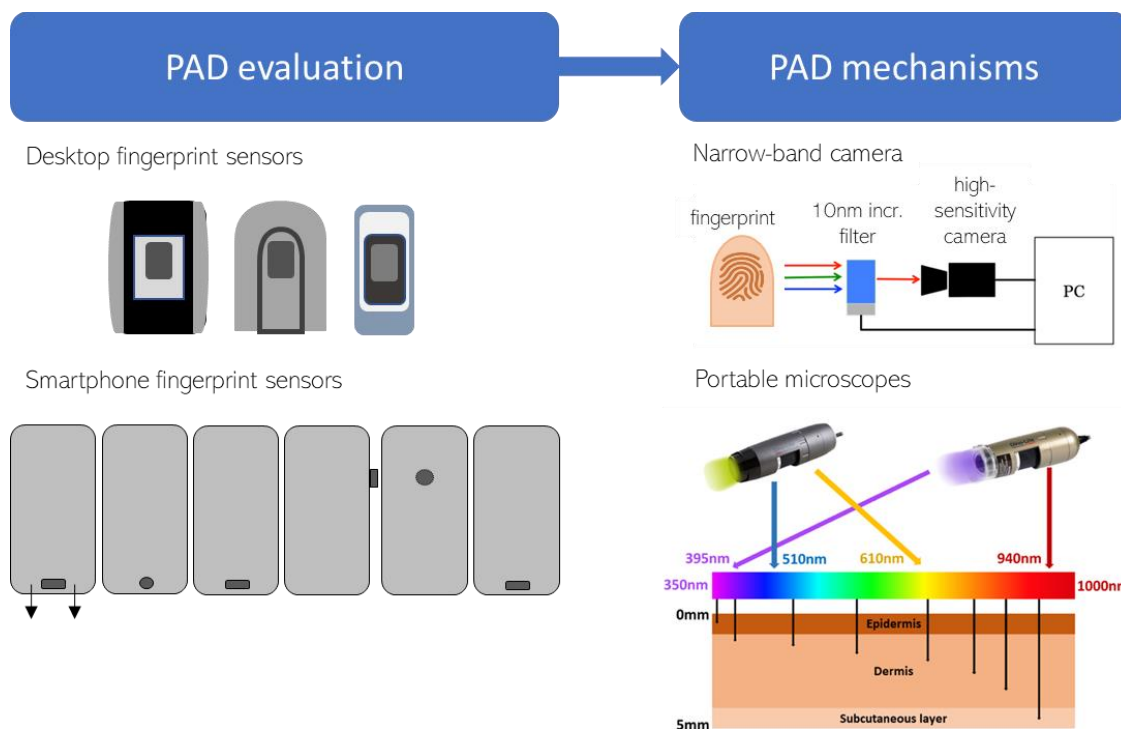
After having two evaluations where biometric experts were attacking mobile devices in a cooperative and non-cooperative manner, the next question arose: "Can non-experts hack smartphone fingerprint sensors, too?" Two different studies (4 and 5) were carried out to answer this question: Study 4 and Study 5.

For study 4, we gave 36 simulated attackers with no background in Biometrics one week to attack one smartphone's fingerprint reader (5 smartphones in total, same ones than in the second study). Each had to, at least, use 3 capture subjects and use each material at least 120 times on the smartphone sensor, making a total of 10,034 attempts. As more than one week would be needed to create non-cooperative fake fingers, the study was focused only on cooperative attacks.

For study 5, we decided to carry out a hackathon of attacking fingerprint readers embedded in mobile devices. 10 attackers with no previous experience in attacking biometric devices were given a week to research attack methods and 12 hours to attack the smartphones. A wide variety of readily available materials (from the supermarket or online marketplaces) were used for creating the artefacts.

After having performed these studies, it was possible to make a comparison of the attack potential for each case and get results, and thus answer if attacking fingerprint sensors is a matter of expertise and how many attempts are needed to successfully attack them, in average.

After commercial desktop and mobile fingerprint readers were evaluated using standards, it was decided to develop a new system to detect fake fingers. For that, this second part of the Thesis focuses on obtaining a low-cost and efficient hardware solution for detecting presentation attacks. With that goal, a pre-study was performed using a narrow-band camera to obtain images of real and fake fingers in 10nm increments of wavelength and, once the images were gathered, different approaches were tried to classify the samples into real or fake fingers. After that, a new approach was developed: 2 handheld microscopes with special lighting were used to perform a PAD (Presentation Attack Detection) evaluation by capturing 7,704 images of fake and real fingerprints of 17 subjects. These images were processed and classified using Bag of Features algorithms, obtaining an attack classification error of 1.78% at 70% training samples (3.99% for 50% training).



**Figure 2. Thesis structure outline.**

This document is divided in 9 chapters: an introduction to biometric recognition, an overview on the state of the art in fingerprint presentation attack detection and vulnerabilities, a description of the methodologies used throughout the Thesis, evaluations, a new system for attack detection and the lessons that were learnt during the process:

**Chapter 2:** This chapter gives an overview on biometric recognition. First, a brief history is summarized, then biometric recognition systems are described and, lastly, there is a subsection on security evaluations on fingerprint biometric systems. This section details all the points where a biometric system can be vulnerable and then focuses on the attack type that is of concern in this Thesis: the presentation attack. Moreover, the international standard that deals with this type of attack is explained in this section, ISO/IEC 30107.

**Chapter 3:** The state of the art of presentation attack detection in fingerprint biometric systems is given in this chapter. It starts with an overview of the most known technologies of fingerprint sensors and then details the state of the art in presentation attack detection evaluations and developed mechanisms.

**Chapter 4:** Once the state of the art and the corresponding standards are explained, this chapter details the methodology that was developed and applied during the experiments of this Thesis. Also, an overview of the different studies is given here for clarification purposes.

**Chapter 5:** This is the first chapter that deals with experiments. In particular, an evaluation is performed with fake fingers on 3 desktop fingerprint readers following ISO/IEC 30107 and the results and conclusions are given.

**Chapter 6:** As a follow-up from the previous chapter, this one deals with PAD evaluations performed on smartphones that have an embedded fingerprint sensor. A methodology for carrying out PAD evaluations on mobile devices is developed and applied here, and an evaluation is performed with cooperative and non-cooperative attacks. Also, a novel and easy method is explained to steal latent fingerprints from smartphone screens.

**Chapter 7:** After having performed attacks on mobile devices by experts, this chapter covers two additional studies but carried out by 48 inexperienced attackers. It tries to answer the question: “does experience count when attacking fingerprint capture devices? Do different attackers with the same knowledge get different results?”

**Chapter 8:** Once several experiments have been performed using fake fingers on desktop and mobile devices, it was decided to develop a new PAD mechanism based on the distinctiveness of skin and fake fingers illuminated by different wavelengths. In this chapter, two approaches are shown: using a narrow-band camera and using special lighting portable microscopes to capture fake and real fingers. An evaluation is performed with both and results and conclusions are given.

**Chapter 9:** Lastly, this chapter gives a closing to the document by noting the lessons that were learnt during the process and suggesting future lines of work.



## Chapter 2. Biometric recognition

---

HUMAN IDENTIFICATION CAN be based on three things, or a combination of them, as IBM said in 1970 [24]:

**What you know.** For instance, a password. A user should have a different one for each application, and they should be complicated enough not to be stolen. That would imply having to remember difficult and long passwords, so a high percentage of users end up setting easy ones.

**What you have.** For instance, an ID card. This removes the problem of forgetting passwords by keeping a card in the wallet, but it adds the possibility of getting stolen or being left somewhere.

**What you are.** For example, a fingerprint. This eliminates the problems of both forgetting and losing something but has its own disadvantages. This will be the topic covered on this Thesis.

Biometric recognition is the identification of an individual by measuring an aspect of his/her biology or behavior. Its three main targets are allowing recognition where human intervention is not possible, avoiding misrecognition due to tiredness and improving the human-machine interaction.

### 2.1 A brief history of biometric recognition

Human recognition goes back in time as much as humans do. We recognize others mainly by the shape of the face, the voice or the behavior. Biometric recognition tries to imitate this ability to identify individuals. Biometrics as a science is considered to

have started when an objective statement of the identity of a person was needed: a handwritten signature, body measurements, fingerprints etc.

Handwritten signature is considered to be the first biometric modality. It was needed to sign documents and other official statements. Those persons who could not write, drew a cross or any other mark.

In the 18<sup>th</sup> century, Thomas Bewick, a British engraver and natural history author, decided to sign his works with his thumb fingerprint [25]. He did not use it scientifically, only for originality or for marketing reasons. The real origin of Biometrics is in 1823, when Joannes E. Purkinje developed a detailed study on ridges and valleys of fingerprints, and classified fingerprints into 9 types [26]. However, fingerprints were not yet adopted as a real mean to identify subjects.

In the last decade of the 19<sup>th</sup> century, Bertillon's identification *anthropometrique* was developed. It was a standard procedure based on taking measurements from the human body, such as the chest, head or feet [27].

Based on Purkinje's studies, in 1858, Sir William Herschel mandated that all Indian natives had to register their hand palms to "avoid dishonesty", but it was meant only to intimidate them [28][29]. Nevertheless, as the database grew, he suspected that palm lines and fingerprints could be unique for each person. Then, during the 1870s, Dr. Henry Faulds began studying the uniqueness and time permanence of fingerprints. He created a classification system and sent it to Sir Charles Darwin, who could not help him and forwarded the information to his nephew, Sir Francis Galton, who did not give it any importance at the beginning.

In the late 19<sup>th</sup> century, Sir Francis Galton performed some studies on fingerprints, based on papers by Dr. Henry Faulds. He demonstrated the uniqueness of fingerprints by estimating the probability of seeing 2 identical fingerprints in 1 over 64 million. He also demonstrated that they remain stable in time and that they are internal features (that is, if a layer of skin is removed, the same shape is shown again). Furthermore, he designed a method for obtaining inked impressions of fingerprints, defined 3 patterns of fingerprints and created a human classification system by using the 10 fingers of a person [30].

In 1894, Scotland Yard decided to complement Bertillon's system with Galton's. On the same year, Sir Edward Henry, Inspector-General of Police of Bengal (India), exchanged letters with Galton due to the problems he was finding when registering the population. He was convinced that the system based on fingerprints was much better than Bertillon's system, decided to take prints of the fingers of all prisoners, and demonstrated that identification based on fingerprints was possible. As a result, he improved the human classification with fingerprints, it became a success in the West Indies and was adopted by Scotland Yard in 1900 [31].

The first attempt to use an automated biometric recognition arose from the need to process fingerprints in the criminal justice system. Historically, an expert had to examine fingerprint images, classify them by patterns and manually compare them to check if there was a match to previously stored images. However, in the early 20<sup>th</sup> century, the number of fingerprint images that needed processing and matching



increased greatly. Hence, an automatic process was highly needed. Soon, other biometric modalities were discovered, studied and developed [32].

Enormous attention was put on Biometrics after the terrorist attacks in the US on September 11, 2001. After this event, biometric recognition systems were introduced at national borders to prevent the use of fake identities from entering the country. In recent years, biometric recognition has widely been introduced in people's lives. Smartphones include it as a comfortable and secure way to be unlocked, as well as computers, and they can be found at gyms or work places for people to get in without the need of a guard checking identities.

## 2.2 Biometric recognition systems

Most biometric recognition systems can be described by the diagram on Figure 3. First, a data capture subsystem is needed to obtain the wanted sample from the sample, it is then stored in the data storage subsystem, compared against previously stored references and, lastly, a decision is made based on the said comparison to check whether it is the correct individual.

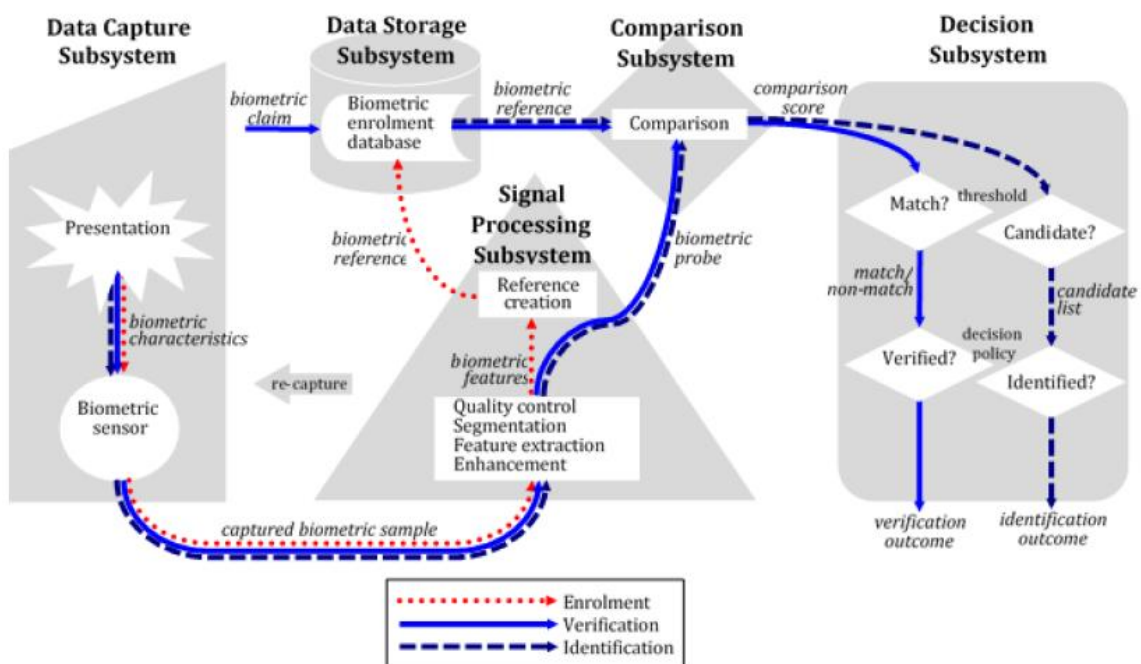
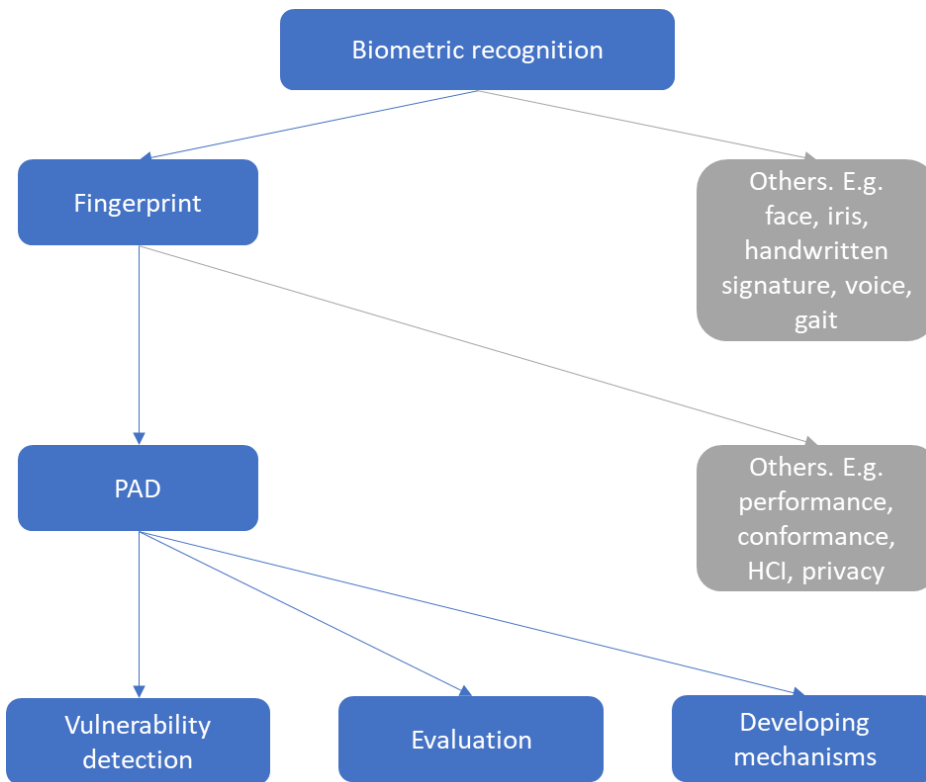


Figure 3. Components of a biometric system [33].

The first step is to capture raw biometric data from a subject (presentation), which is done through a sensor by translating it into a digital sample. No two samples will ever be the same, as no presentation can ever be done equally twice. Then, the sample is processed to extract needed features. In face recognition, the eyes need to be found; in fingerprints, minutiae (ridge endings or bifurcations). In this stage, the quality of the sample is analyzed. If the quality is too poor, a re-capture will be done. Once the quality is good enough, a reference is created and stored in a database. This is called *enrollment*.

Once a subject has been enrolled, two types of recognition can be done: *verification* and *identification*. Verification is the process to check if the subject is who he or she claims to be. It is a 1:1 comparison, because it compares the presented sample to the subject’s previously stored sample. An example of this is a user who wants to unlock his or her phone with the fingerprint. Identification is the process of locating a subject among an entire database of previously enrolled users. It is, thus, a 1:N comparison. It is used mainly for forensics, for victim or criminal identification.

Although biometric recognition entails many different modalities (e.g. fingerprint, iris, face, handwritten signature, gait), this Thesis will focus on fingerprint recognition, as it is widely used in access control and, increasingly nowadays, smartphone unlocking. In order to ensure the intended operation of the biometric application, it is necessary to evaluate the systems. These can undergo several different types of evaluations: performance, conformance, security, human computer interaction, privacy, etc. This work will focus on presentation attack detection (PAD) evaluations, which are part of security evaluations (Figure 4).



**Figure 4. Diagram of the focus of this Thesis.**

### 2.3 Security evaluation of fingerprint biometric systems

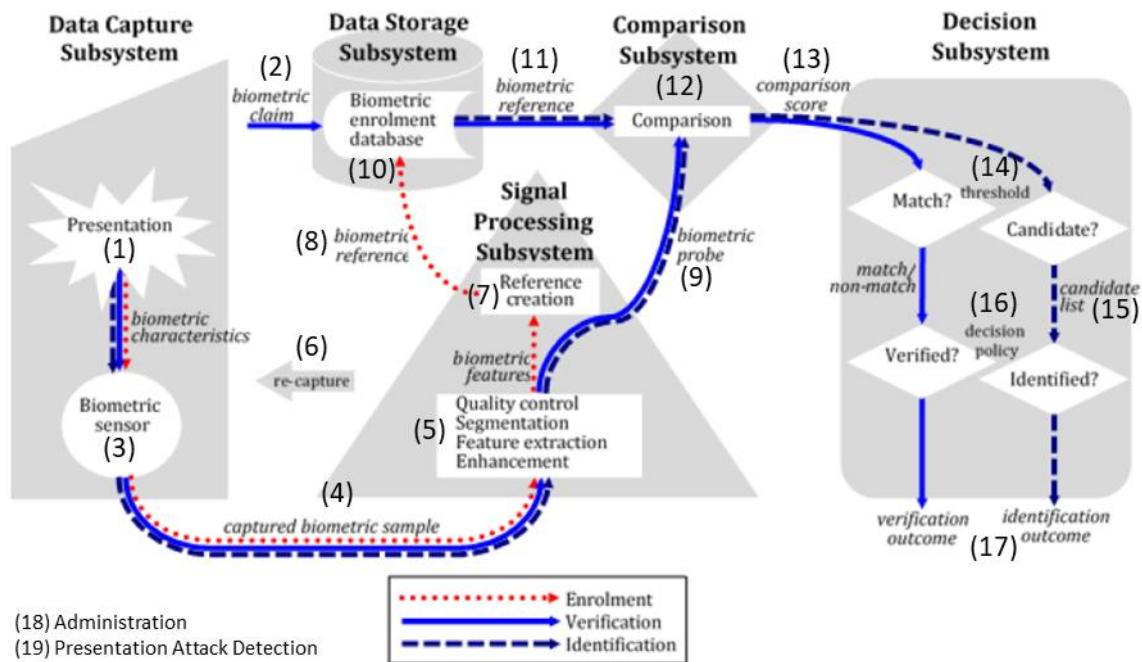
This section will give an overview of security evaluation on fingerprint biometric systems, which is the focus of this Thesis, as it was noted on the last section. This will be divided into general vulnerability points in a biometric system and then it will be narrowed down to presentation attack detection evaluation according to its corresponding standard, ISO/IEC 30107.

### 2.3.1 Vulnerabilities in fingerprint biometric recognition

Biometrics is entirely based on probability. Every time an individual presents a sample to the system, the captured information will be different for several reasons: behavior of the subject, movement, environmental conditions or physical aging. That is, a system can never be absolutely sure of a subject's identity.

The vulnerability of a system is a different concept from the accuracy of a system. A system can be very accurate, meaning that it can distinguish well between two individuals, but it can be highly insecure. Over the years, focus has been put mainly on improving accuracy (performance), while the assessment of vulnerabilities has been overlooked. Knowing and studying a system's vulnerabilities is becoming more crucial as Biometrics' use increases (cellular phones, computers, access control, etc.).

Figure 5 shows that a biometric system is composed by several connected subsystems, each with its own point of attack. These can be exploited in the following manners:



**Figure 5. Vulnerability points in a biometric recognition system [33].**

1. **Presentation:** A fake biometric trait is presented, or a real subject modifies the sample to make it seem like another (for example, using makeup). Also, the real subject might be forced to use his or her biometric trait unwillingly.
2. **Biometric claim:** The use of a fake or stolen identifier to create a false claim of identity. For example, an attacker who creates a fake ID and then proceeds to get a fake identity at a government office with his or her fingerprint.
3. **Biometric sensor:** Faking the sensor. The signal processing subsystem should be able to check the integrity of the reader by cryptographic techniques. For example, a computer camera can be replaced with a different one that always sends the same image [32].

4. **Captured biometric sample:** data can be intercepted for later use if the connection is not secure. Also, a fake biometric sample can be substituted for the real one.
5. **Quality control, enhancement and feature extraction:** In enrollment, if a low-quality sample is used, it can be easier to attack afterwards.
6. **Re-capture:** Allowing many capture trials lets the attacker learn which attack methods work best on the system.
7. **Reference creation:** Reference generation code can be modified in order to suit the attacker's needs to enter the system.
8. **Transmission – Reference to enrollment:** if the channel is insecure, enrollment data can be substituted before it reaches the database
9. **Transmission – Features to database:** as in the previous case, if the channel is insecure, the sample could be substituted before it is stored.
10. **Biometric enrollment database:** this is the source of authentication data. If it is compromised, modifications and substitutions could occur.
11. **Transmission – Reference from database:** if the channel is insecure, an attacker could substitute references before they are compared.
12. **Comparison process:** this process generates a similarity score with the sample and the reference template. This could be compromised, giving high scores to the wanted samples.
13. **Transmission – score:** if not transmitted securely, the score can be modified.
14. **Threshold process:** the match threshold could be modified and set to any value, so that attackers could be accepted easily by the system.
15. **Candidate list:** it can be modified so that the individual the attacker chooses does not appear on the list.
16. **Decision policy:** it uses rules to give a final acceptance or rejection based on the match results. An attacker could modify it and make his or her own acceptance decisions.
17. **Transmission – Outcome:** the outcome is transmitted to take action (unlocking a door, for example). If it is compromised, the outcome could be changed.
18. **Administration:** a malicious administrator can substitute enrollment data or reduce thresholds so that attackers can pass under a false identity.
19. **Presentation attack detection:** presentation attack detection can be used to protect against artefacts. It can also be open to attack: a fingerprint system can use heat for presentation attack detection, and an attacker can warm an artefact to fool it.

Of all the points of attack mentioned above, attacks at the presentation level are the ones that will be researched in this work. Namely, presentation attacks.

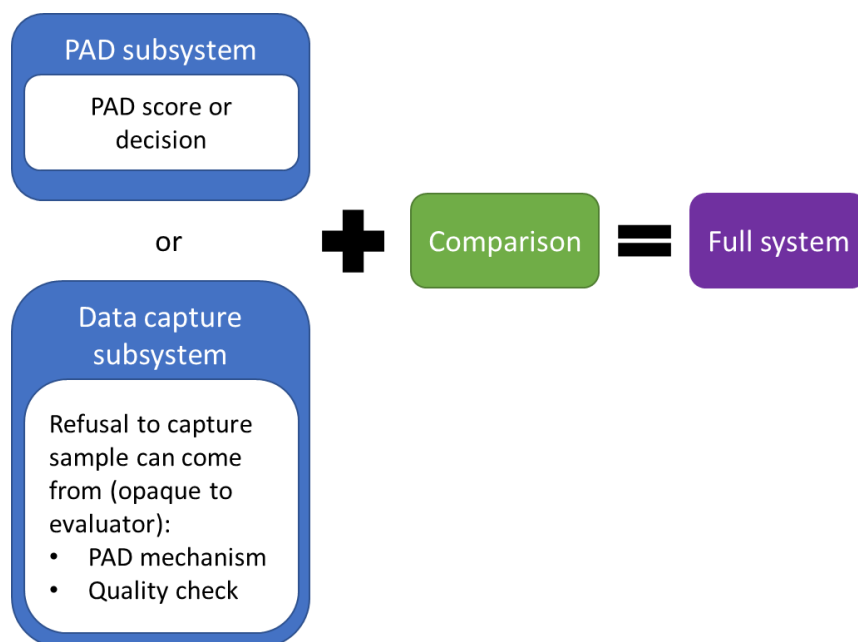
### 2.3.2 Presentation attack detection evaluation (ISO/IEC 30107)

The standard that focuses on evaluating vulnerabilities at the presentation attack level is ISO/IEC 30107 – *Biometric presentation attack detection*. The parts that are of concern for this Thesis are Part 3: *Testing and reporting* and Part 4: *Profile for evaluation of mobile devices*. They address techniques for the automated detection of presentation attacks, namely presentation attack detection (PAD) mechanisms, and Part 4 focuses on mobile devices, which have some distinct characteristics when being evaluated.

According to this standard, a presentation attack is the *presentation of an artefact or of human characteristics to a biometric capture subsystem in a fashion intended to interfere with system* [1]. As is the case for biometric recognition in general, PAD mechanisms are subject to false positive and false negative errors for both bona fide and attack presentations. Bona fide presentations refer to the interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system, while attack presentations refer to presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system [1]. Errors when classifying both types can lead to flagging or inconveniencing legitimate users or security breaches.

All evaluations of PAD mechanisms are determined by the item under test (IUT). The IUT is categorized as follows (a diagram of all systems can be seen on Figure 6):

- **PAD subsystem:** hardware and/or software that implements a PAD mechanism and makes an explicit declaration regarding the detection of presentation attacks. Results of the PAD mechanism are accessible to the evaluator and are an aspect of the evaluation.
- **Data capture subsystem:** consisting of capture hardware or/and software, it couples PAD mechanisms and quality checks in a fashion opaque to the evaluator. The evaluator may not necessarily know whether the data capture subsystem utilizes presentation attack detection. Acquisition may be for the purpose of enrollment or recognition, but no comparison takes place in the data capture subsystem.
- **Full system:** adds biometric comparison to the PAD subsystem or data capture subsystem, comprising a full end-to-end system. This leads to additional failure points for the Presentation Attack Instrument (PAI) beyond PAD mechanisms and quality checks. In a full system, there might be one or multiple PAD mechanisms at different points in the system.



**Figure 6. Diagram of categories of the IUT (Item Under Test).**

Depending on the type of system or subsystem, different metrics will be of interest. In this work, full systems and PAD subsystems will be addressed. According to the standard, these are the relevant metrics for each case:

- PAD subsystem:
  - **APCER** (Attack Presentation Classification Error Rate): proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario.
  - **BPCER** (Bona-fide Presentation Classification Error Rate): proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario.
- Full system:
  - **IAPMR** (Impostor Attack Presentation Match Rate): full-system evaluation of a verification system proportion of impostor attack presentations using the same PAI species in which the target reference is matched.
  - **APNRR** (Attack Presentation Non-Response Rate): proportion of attack presentations using the same PAI species that cause no response at the PAD subsystem or data capture subsystem.
  - **APAR** (Attack Presentation Acquisition Rate): proportion of attack presentations using the same PAI species from which the data capture subsystem acquires a biometric sample of sufficient quality.

This Thesis will deal with PAD evaluations only, not performance ones. For further information on performance evaluations, there is extensive work carried out by Tony Mansfield, Jim Wayman or Belen Fernandez-Saavedra. Information on how to carry out performance evaluations is gathered on the standard ISO/IEC 19795 - *Information technology – Biometric performance testing and reporting* [33]. Within PAD evaluations, both full systems (desktop and mobile devices with a fingerprint sensor) and PAD subsystems (PAD mechanisms that were developed) will be covered in this Thesis.

## Chapter 3. State of the art

---

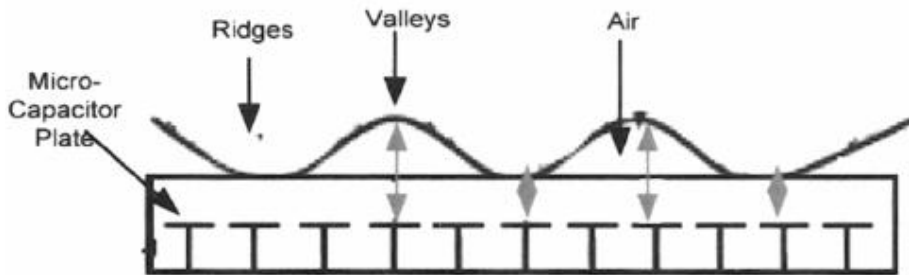
THIS SECTION WILL give a walkthrough on the state of the art of presentation attacks for the fingerprint modality. Firstly, details will be given on different techniques to attack fingerprint readers and the PAD evaluations that were performed in the literature. Secondly, an overview of the PAD mechanisms for the fingerprint modality will be detailed.

### 3.1 Fingerprint sensors

This subsection explains the most known and used fingerprint sensor types and gives the characteristics of the scanners that were used for this work. This is essential for understanding how fake fingers can fool the them. There are many types of fingerprint scanners: capacitive, radiofrequency, optical, thermal, piezo resistive, ultrasonic etc., but this subsection will only focus on the three most used technologies: capacitive, optical and thermal readers. All fingerprint sensors measure physical properties from a finger and transform them into a digitalized image of its ridge and valley patterns.

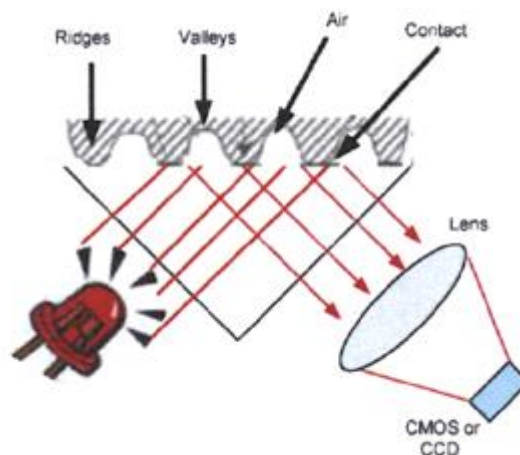
**Capacitive sensors** use a matrix of capacitors to get an image of the skin, which is conductive. One of the capacitor plates is on the device and finger skin acts as the other plate [34]. The sensor sends a small voltage to the finger in order to measure the capacitance. This capacitance is different between ridges and valleys, because the former have a higher capacitance than the latter [7]. This way, an image can be generated Figure 7.

There are two kinds of capacitive readers: active and passive. The difference between them is that the required initial voltage excitation on the skin for active sensors needs twice the current draw of the passive ones [35].



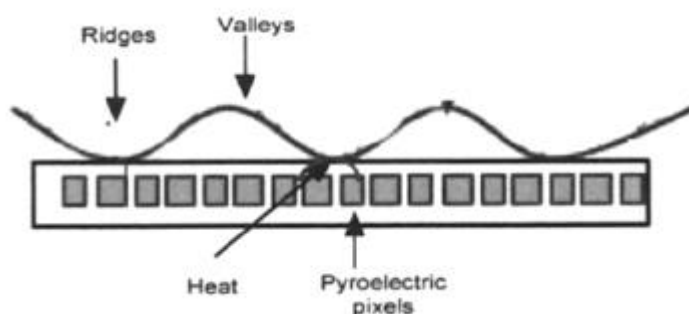
**Figure 7. Capacitive fingerprint sensor** [34]

**Optical sensors** use a matrix of CMOS sensors. The finger is pressed against a transparent plate and then illuminated. Through lenses, the image is projected and then grabbed by the CMOS sensors [7], generating an image from the fingerprint.



**Figure 8. Optical fingerprint sensor** [34]

**Thermal sensors** use a matrix of temperature sensors formed by a pyro-electric material [36]. The temperature of the skin (ridges) and the temperature of the air (valleys) is different, and the sensors read and process it to get an image [7] (Figure 9).



**Figure 9. Thermal fingerprint sensor** [34]



### 3.2 Presentation attack detection evaluation

Once the fingerprint sensors' technologies are known, attacks can be designed to exploit the specific technology. Optical readers will be vulnerable to non-translucent fake fingers; capacitive ones, to materials that are conductive; thermal, to materials that are not thermal isolators.

Fingerprint systems have previously been spoofed with fake artefacts made from molds from real fingers, both with the subject's consent and without. Several materials that have properties similar to human skin (i.e. conductance, elasticity, humidity) have been found to fool the recognition system [10], [12], [13], [37]–[39]. Already in 1990, several sensors started being tested using artefacts, and the system failed to reject them even from the first attempt [7]. On 2000, an evaluation was performed on [13] by calculating the acceptance rate of 1 user's finger made with gelatin on 11 readers, where the artefacts were accepted by the systems in a very high percentage (the lowest being 67% fake finger acceptance rate). On 2002, several more attacks were demonstrated by using latent fingerprint reactivation on 6 capacitive, 2 optical and 1 thermal scanners [40]. For the case of [10], 10 subjects were used to create gelatin fingers and use them on 3 capture devices, getting success rates from 44.6% to 76%. On all experiments, only index fingers were used. In general, nevertheless, these studies do not follow a thorough evaluation procedure nor standard, and merely prove when a certain material or technique is effective on specific sensors at least once. The few evaluations where numerical results were reported are represented on Table 1. The results marked with a \* refer to results that were reported in graphs with no exact numbers.

In 2009 [41], Liveness Detection (*LivDet*) competitions started and continued on 2011 [39], 2013 [42] and 2015 [43]. Their goal was to compare different liveness detection (Presentation Attack Detection) mechanisms by using them on a very large database of fake fingers (made of gelatin, latex, ecoflex, Play-Doh, silicone, wood glue and modasil). Different academic institutions or industries could try their algorithms on the database. Four different sensors were used to acquire the images and the evaluations were done using a common testing protocol.

To the authors' knowledge, there have not been evaluations specifically focused on attacking mobile devices with fake fingers, but there have been reports on found vulnerabilities. In 2013, when the first iPhone with an integrated fingerprint reader came out, the Chaos Computer Club [16] proved that it was possible to break into the device using a white glue fake finger covered with graphite, and the fingerprint could be stolen from the phone screen using a scanner and doing some image processing. Nonetheless, this was only reported once in a video, not in a complete evaluation. In 2016, fake fingers were printed using conductive ink (having a sample of the fingerprint image beforehand), so they could be used directly on the mobile phone sensor without having to create molds previously [44]. This was a technical report to inform about the vulnerability, and not an evaluation.

**Table 1. IAPMR results and characteristics of each evaluation. Only experiments with reported numerical results are shown.**

Evaluation	Year	Sensor technology	Cooperation	Capture subjects	PAI species	Attempts	IAPMR (%)
T. Matsumoto et al. [13]	2002	Optical	Cooperative	5	Gelatin	100	98*
		Optical				100	71*
		Optical				100	81*
		Optical				100	98*
		Optical				100	90*
		Capacitive				100	84*
		Capacitive				100	75*
		Capacitive				100	91*
		Capacitive				100	79*
		Optical				100	84*
		Optical	100	80*			
		Optical	Non-cooperative	1	Gelatin	100	100*
		Optical				100	95*
		Optical				100	100*
		Optical				100	100*
		Optical				100	79*
		Capacitive				100	97*
		Capacitive				100	100*
		Capacitive				100	92*
		Capacitive				100	79*
Optical	100	100*					
Optical	100	100*					
J. Blommé [10]	2003	Capacitive	Cooperative	10	Gelatin	500	55.4
		Optical				500	34.4
		Capacitive				500	24
A. Wiehe et al. [12]	2004	Optical	Cooperative	1	Silicone	10	100
					Gelatin	10	0
		Capacitive	Cooperative		Silicone	10	0
					Gelatin	10	0
		Optical	Non-cooperative		Wood cement	10	100
		Capacitive	Non-cooperative		Gelatin	10	0
M. Sandstrom et al. [45]	2004	Optical	Non-cooperative	3	Gelatin	150	88.5*
		Electric field				150	92.5*
		Electric field				150	47*
S. Elliott et al. [46]	2007	Optical	Cooperative	1	Gelatin	163	90.7
S. Schuckers et al. [39], [41]–[43]	2009, 2011, 2013, 2015	LivDet competitions. Various results, see Table 2					

### 3.3 Presentation attack detection mechanisms

Numerous approaches have been studied and implemented to overcome presentation attacks on fingerprint biometric systems [47], divided into software and hardware mechanisms. On the software side, there are static methods (sweat pore detection [48]–[50], ridge and valley [51]–[53], perspiration [54], [55], etc.) and dynamic methods (skin distortion [56], [57], perspiration [58]). For the hardware approach, research has been made on challenge/response [59], odor [60], pulse oximetry [61], multispectral imaging [62]–[64] and OCT [65]–[67], among others.

Based on the standard ISO/IEC 30107-3, the IUT (Item Under Test) shall be categorized into the PAD subsystem, data capture subsystem and full system, as explained previously on subsection 2.3.2. For PAD mechanisms, the pertinent block is the PAD subsystem, that is, hardware and/or software that implements a PAD mechanism and makes an explicit declaration regarding the detection of presentation attacks.

The metrics that concern us for this literature analysis are the proportion of misclassifications of attack and bona fide presentations, that is, APCER (Attack Presentation Classification Error Rate) and BPCER (Bona fide Presentation Classification Error Rate), respectively. Two tables (Table 2 and Table 3) were filled gathering the state-of-the-art results for APCER and BPCER, whenever possible, because many studies do not give results according to the standard, and others do not report numerical results at all. Also, the materials used for creating the fake fingers are detailed.

**Table 2. Software PAD performance with independent evaluators. Results were gathered from [47].**

Algorithm/author	PAI species	APCER (%)	BPCER (%)
Dermalog [41]	Gelatin, latex, Play-Doh, white glue, silicone, ecoflex	5.4	20.1
ATVS [41]		9.0	30.1
Anonymous [41]		16.0	32.8
Anonymous2 [41]		16.0	13.2
Dermalog [39]	Gelatin, latex, Play-Doh, white glue, silicone, ecoflex	0.8	42.5
Greenbit [39]		39.5	38.8
Federico [39]		24.5	26.6
CASIA [39]		24.8	29.63
LBP pores detection [68]		11.13	13.30
Power spectrum [68]		24.65	41.40
Wavelet energy [68]		39.03	27.53
Ridges wavelet [68]		41.34	30.58
Valleys walevet [68]		38.81	10.08
Curvelet energy [68]		40.70	31.08
Curvelet GLCM [68]	22.15	27.88	

**Table 3. Software PAD performance with self-declared results and evaluations. Results were gathered from [47].**

Algorithm/author	PAI species	APCER (%)	BPCER (%)
Nikam and Agarwal [69]	Gelatin, Play-Doh, plastic, silicone sealant, Putty, alginate	2.08	1.62
Nikam and Agarwal [70]	Gelatin, Play-Doh	2.5	2.16
Nikam and Agarwal [71]	Gelatin, Play-Doh	2.5	2.16
Espinoza and Champod [48]	Latex	21.2	8.3
Galbally et al. [72]	Gelatin, Play-Doh, silicone	6.27	6.85
Pereira et al. [73]	White glue, silicon	3.47	10.52
Marasco and Sansone [53]	Gelatin, latex, Play-Doh, white glue, silicone, ecoflex	12.3	12.63
Nikam and Agarwal [74]	Gelatin, Play-Doh	3.33	1.62
Nikam and Agarwal [75]	Gelatin, Play-Doh	3.33	1.62
Tan and Schuckers [51]	Gelatin, Play-Doh	6.0	2.28
Marasco and Sansone [76]	Gelatin, latex, Play-Doh, white glue, silicone, ecoflex	12.3	12.63
Decann et al. [77]	Gelatin, Play-Doh, silicon	1.2	1.2
Tan and Schuckers [55]	Gelatin, Play-Doh, silicon	0.9	0.9
Nikam and Agarwal [78]	Gelatin, Play-Doh	0.9	2.08
Jia and Cai [79]	Gelatin	4.49	4.49
Antonelli et al. [56]	Gelatin, latex, white glue, RTV silicon	11.24	11.24
Zhang et al. [57]	Silicon	4.5	4.5
Jia et al. [80]	Gelatin	4.78	4.78

As it can be noticed, results that are self-reported have much lower error rates than those that went through an independent evaluation using the same methods. The average APCER for the independent evaluations of software solutions is 31.12%, while the BPCER is 25.98%. On the other hand, the APCER average for self-declared results is 5.74% and the BPCER is 5.09%.

On the hardware side, there are scarce reports on results, few databases exist and those that do are very small. In these cases, the evaluation results have been self-declared. APCER and BPCER (whenever possible to find) are shown on Table 4.

**Table 4. Hardware PAD performance.**

Hardware method	Authors	PAI species	APCER (%)	BPCER (%)
OCT	Cheng and Larin [81], [82]	White glue, silicon, household cement	-	-
	Sousedik, Breithaupt, Busch [83]	Glycerol, graphite, window paint	11.32 (50% T) 6.17	3.52 (50% T) 25.37
	Menrath and Breithaupt [84]	?	-	-
	Nasiri-Avanaki et al. [67]	Sellotape	-	-
Challenge-response	Wei-Yun et al. [59]	Gelatin	0	0
Odor analysis	Baldiserra et al. [60]	Gelatin, latex, RTV silicon	-	-
Pulse oximetry	Reddy et al. [85]	Gelatin, Play-Doh	0	0
	Hengfoss et al. [86]	Cadaver	-	-
Multispectral	Ratha and Govindaraju [64]	Gelatin, gold latex, clay, green gummy	-	-
	Lumidigm	Silicon	-	-
	Chang et al. [87]		-	-

Those results that show a zero percent error rate are probably due to not having done an extensive evaluation, but only a concept proposal and trial with few users. Studies on Optical Coherence Tomography (OCT) have been more complete and, in general, adapted to ISO/IEC 30107-3. Although some reports show promising results for such technologies, there are some drawbacks:

- **OCT:** expensive (thousands of euros), needs a few seconds to capture the fingerprint (0.02s for a genuine finger [88] or up to 56s for another case [84]) and the finger has to stay very still because it is easy to get disturbances. There are two commercial products from IDEMIA [89] and THORLABS [90], but no evaluation results are published.
- **Challenge-response:** in this case, the user is given a tactile pattern on the reader surface and he/she needs to identify the pattern as a response. The problem is that the system is difficult to use, as the user cannot reliably perceive the proposed pattern. Also, it is uncomfortable for the user due to the currents sent to the finger.
- **Odor analysis:** although it works well with fake finger materials like silicone, others are difficult to identify because the sensor's response is similar to that obtained in the presence of human skin (for instance, with gelatin).
- **Pulse oximetry:** users must hold their finger for up to four seconds until the pulse sample is obtained and it does not work with thin materials, as pulse can be transmitted.
- **Multispectral:** although it has been claimed that this solution is very efficient, this present work shows that only one wavelength may be enough to distinguish fake from real fingerprints, simplifying the hardware needed. Also, the solutions noted on Table 4 are commercial and not academic, so the results are not public.



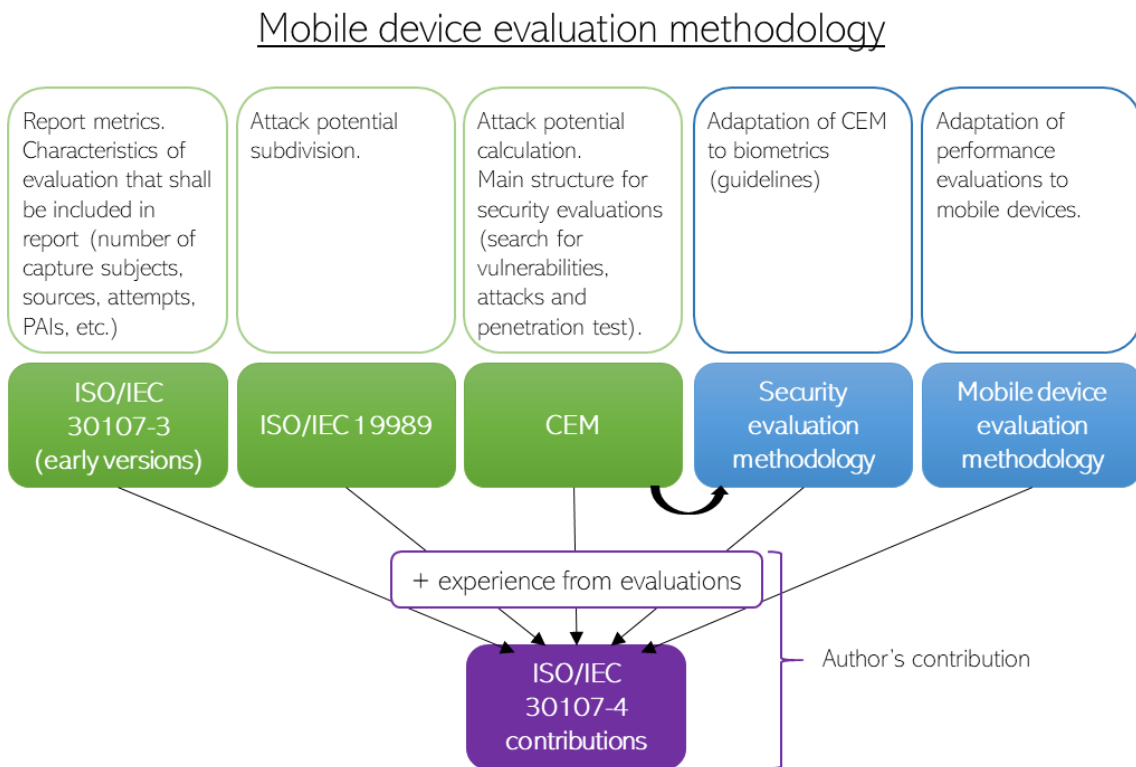
## Chapter 4. Presentation Attack Detection evaluation methodology and studies

---

AS IT WAS mentioned in previous sections, there are currently tools and methodologies to perform PAD evaluations, such as the standards ISO/IEC JTC1/SC37 30107 [1], [2] and ISO/IEC JTC1/SC27 19989 [91] or Common Criteria's Common Evaluation Methodology (CEM) [18]. The PAD experiments carried out during this Thesis cover desktop and mobile device fingerprint sensors. Both cases have inherent differences, so the PAD evaluation methodology slightly differs for each case. For the case of desktop readers, ISO/IEC 30107 Part 3 – *Testing and reporting* was used to report the obtained results. Although at this moment there exists a new part of that standard dedicated especially for mobile devices (Part 4 – *Profile for evaluation of mobile devices*), there was not at the time of performing the experiments of this Thesis and reporting them. Thus, a new methodology was designed and applied with the purpose of bringing PAD evaluation to the case of mobile devices, which is the focus of this chapter. This became a contribution to the said standard.

The main structure of the methodology stems from Common Criteria, as it was gathered in a best practices document [19], where the security issues were adapted due to the inherent nature of biometric recognition systems. Moreover, the attack potential concept was also taken from CEM [18] and subdivided into more specific steps based on ISO/IEC 19989 [91]. ISO/IEC 30107 – *Biometric presentation attack detection* [1] was in an early stage when this work started, but it already included many useful report metrics and report factors that shall be included in a PAD evaluation. Nevertheless,

some aspects of this standard could not apply to mobile devices, mainly because the evaluator does not have access to decision policies on scores, quality, transactions, etc. Thus, some characteristics from a work on performance evaluation focused on mobile devices [21] were also added to the final methodology. A combination of the aforementioned best practices, standards and methodologies plus the experience gained on performing evaluations gave way to the methodology proposed on this Thesis by the author. Moreover, these contributions were discussed and accepted in the new part of standard ISO/IEC 30107, Part 4: *Profile for evaluation of mobile devices*. The influences of each methodology and standard are shown on Figure 10.

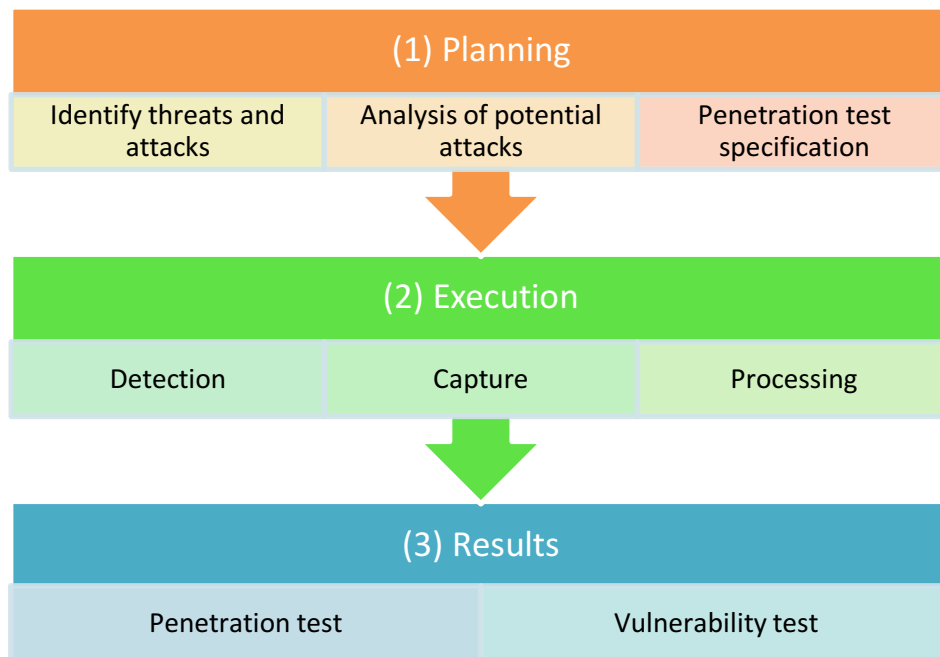


**Figure 10. New methodology developed for testing PAD in mobile devices.**

The resulting methodology will be detailed along this chapter and, as it will be seen in Chapter 5, Chapter 6 and Chapter 7, it will be followed on every PAD evaluation on desktop and mobile devices.

First, as for every security evaluation according to Common Criteria, three steps are needed: planning, execution and results reporting. Each of them entails a subset of phases, gathered in Figure 11. These will be detailed in the upcoming subsections of this chapter.





**Figure 11. Steps needed for biometric evaluations.**

## 4.1 Planning the evaluation

When planning a PAD evaluation, specific steps should be made, as detailed as possible, so that the later execution runs smoothly. Evaluators need to make sure that they have considered as many details as possible. For this end, three steps are needed: identification of all possible threats and attacks that may exploit the vulnerabilities of the system, analysis of potential attacks and specification of penetration test.

### 4.1.1 Identification of all possible threats and attacks

The steps that shall be followed to identify all possible threats and attacks to the system are: description of the Target of Evaluation (TOE), description of the target application, search of possible threats and definition of the corresponding attacks.

#### 4.1.1.1 Description of TOE (Target of Evaluation)

The first step of this phase is to describe the system that will be put to the test. Thus, the Target of Evaluation (TOE) should be described in terms of:

- Type of biometric system and its elements (Figure 6). The relevant characteristic in this case is the level of evaluation of the PAD mechanism. According to ISO/IEC 30107-3, these can be PAD subsystem, data capture subsystem or full system. These were detailed on 2.3.2.
- Characteristics such as modality, sensing technology and/or type of algorithm.

#### 4.1.1.2 Description of target application

A PAD evaluation has no meaning or purpose unless the target evaluation and the conditions under which it is performed are specified, as they are key elements to search and classify possible threats and corresponding attacks. Thus, the following descriptions are needed:

- Target application and elements and conditions of the operational environment. A distinction between impostor (subject intends to be recognized as a specific, targeted individual known to the system) and concealer (attacker seeks to conceal his/her own biometric characteristics) attacks is relevant here. Conditions in a mobile device access or in an Automatic Border Control (ABC) system are different: for the former, it is an impostor attack case, as the attacker tries to access a phone that does not belong to him or her by reproducing the owner's biometric characteristics; for the latter, both cases could happen, as the attacker could try to impersonate someone else, or he/she could try to conceal their real fingerprints to avoid a black list he/she is a part of.
- Implemented functions and their policies: enrollment, verification and/or identification. The policies can cover number of allowed presentation attempts, maximum duration or decision-making after all attempts have failed.

#### 4.1.1.3 Search of threats and corresponding attacks

Based on the description of the TOE and the target application, threats and attacks can be found. Every threat has at least one corresponding possible attack [18] and they shall be analyzed before defining the penetration test.

##### 4.1.1.3.1 Search possible threats

Desktop and mobile device fingerprint sensors can have vulnerabilities at many points, and they shall be analyzed. For that, the evaluator should study the intended operation of the system and then think how an attacker could manipulate and take advantage of it. The only vulnerable point used for the scope of this Thesis is the capture process (attack presentations).

##### 4.1.1.3.2 Define possible attacks

After the possible threats have been found, the corresponding attacks can be determined. These attacks shall be described in detail (for this case, source of the biometric characteristic, methods to create the mold and the artefact), following ISO/IEC 30107 Parts 3 [1] and 4 [2]. In this scope, the attack that can exploit the threat explained in the previous point is the presentation attack, i.e., using an artefact generated from a user's real finger. The biometric characteristic can be obtained in two ways: with or without cooperation from the capture subject, namely, cooperative and non-cooperative attacks.

In addition, the expertise of the attacker and effort expended in preparing and performing the attacks shall be specified, but this matter will be detailed in the next section covering attack potential calculations.

#### 4.1.2 Analysis of potential attacks

The Attack Potential is a standardized measure given by Common Criteria. According to Common Criteria methodology [18], the attack potential is a measure of the *effort to be expended in attacking a TOE (Target of Evaluation) with a PAI (Presentation Attack Instrument), expressed in terms of an attacker's expertise, resources and motivation*, which can be divided into more specific parameters. Thus, TOEs are given a rating to assess their resistance to specific attacks.

A score can be assigned to each of the mentioned parameters following CEM's table (Table 5). By adding all the values from the different parameters, the attack potential of an PAI species is rated as Basic, Enhanced-Basic, Moderate, High or Beyond high (Table 6). Once this rating is known, the corresponding attack resistance can be obtained (No rating, Basic, Enhanced-basic, Moderate or High).

**Table 5. Calculation of attack potential. Each category is assigned a value according to this table [18].**

<b>Factor</b>	<b>Value</b>	<b>Factor</b>	<b>Value</b>
<b>Elapsed time</b>		<b>Knowledge of TOE</b>	
<= 1 day	0	Public	0
<= 1 week	1	Restricted	3
<= 2 weeks	2	Sensitive	7
<= 1 month	4	Critical	11
<= 2 months	7	<b>Window of opportunity</b>	
<= 3 months	10	Unnecessary / unlimited access	0
<= 4 months	13	Easy	1
<= 5 months	15	Moderate	4
<= 6 months	17	Difficult	10
> 6 months	19	None	
<b>Expertise</b>		<b>Equipment</b>	
Layman	0	Standard	0
Proficient	3	Specialized	4
Expert	6	Bespoke	7
Multiple experts	8	Multiple bespoke	9

**Table 6. Rating of vulnerabilities and TOE resistance [18].**

<b>Values</b>	<b>Attack potential required to exploit scenario:</b>	<b>TOE resistant to attackers with attack potential of:</b>
0 – 9	Basic	No rating
10 – 13	Enhanced-basic	Basic
14 – 19	Moderate	Enhanced-basic
20 – 24	High	Moderate
=> 25	Beyond High	High

Once the attacks are defined, the penetration test can be designed as a conclusion to the evaluation planning.

### 4.1.3 Specification of penetration test

The penetration test shall describe the complete procedure to conduct each attack. In this case, ISO/IEC 30107-3 [92] gives guidelines on which information must be included, namely:

- number of presentation attack instruments, PAI species, and PAI series used in the evaluation;
- number of test subjects involved in the testing, including those unable to utilize artefacts or present non-conformant characteristics;
- number of artefacts created per test subject for each material tested;
- number of sources from which artefact characteristics were derived;
- number of tested materials;
- description of output information available from PAD mechanism;
- ordering of subject presentations with and without PAI, and whether subjects were reused; and
- ordering of subject presentations to the PAD enabled and disabled system, and whether subjects were reused.

## 4.2 Execution of the evaluation

After the careful planning of the evaluation, it can be finally executed. For that, different penetration tests need to be carried out and, as it was mentioned previously, in this Thesis we will focus on presentation attacks. The biometric system shall be attacked as many times as addressed in the previous phase. The execution has three phases: detection, capture and processing.

### 4.2.1 Detection

Several trials should be made with different materials to check if the sensor can detect the artefact. If it does, then the material can be selected for the evaluation. Although, if there is any sign that a modification to the artefact or presentation method could work, the evaluator shall try to find it. If the evaluator realizes that some specific behavior helps the artefact to get through the system, it should be applied to the rest of the evaluation [92]. Hence, the evaluator can improve his or her skills during the evaluation.

### 4.2.2 Capture

In the same way as in the detection phase, if the system provides any indication that the PAI is being captured successfully, evaluators must analyze the situation and consider whether a modification to the building process or usage could improve the attack successes. If it does, the procedure should be applied to the rest of the penetration test.

### 4.2.3 Processing

As the last step, evaluators shall check whether the system is able to process the acquired sample, that is, whether features can be obtained from it and can be compared

to one or more samples (verification or identification, respectively). These can be quality results, similarity scores or pass/fail results.

### 4.3 Results reporting

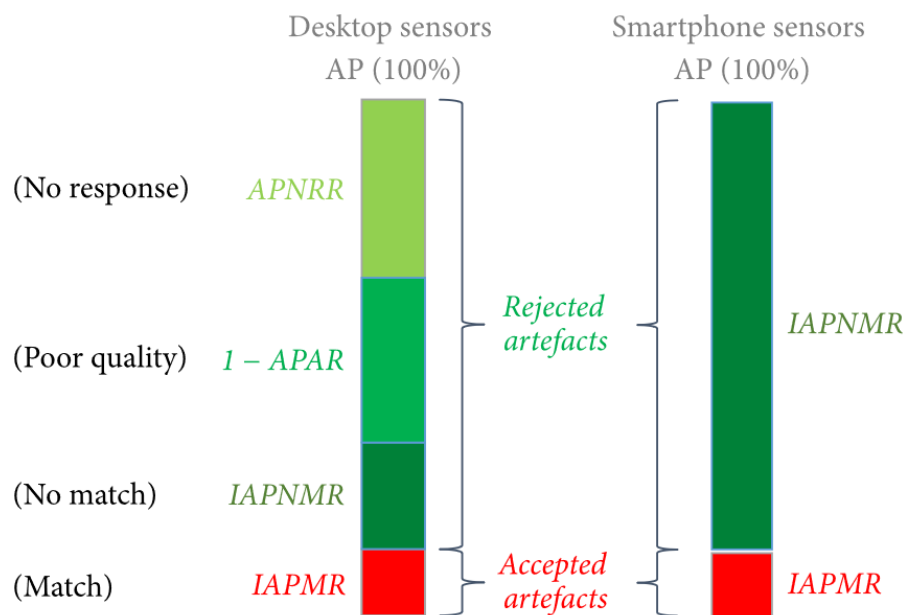
Lastly, once the evaluation has been executed, all the gathered data should be put together and analyzed. Also, based on the outcomes that arose from the penetration test, a list of vulnerabilities shall be reported, along with the consequences that may derive from successful attacks.

#### 4.3.1 Vulnerability test results

Once all the data has been analyzed for the penetration test, the evaluator shall report which PAI species were successful on each specific device to report their vulnerabilities to presentation attacks. Also, the consequences that may derive from a successful attack shall be explained.

#### 4.3.2 Penetration test results

As explained on 2.3, the standard ISO/IEC 30107-3 requires specific reporting metrics for PAD evaluations. On the experiments of this Thesis, the possible metrics are APNRR, APAR, and IAPMR, depending on the level of access of the evaluator (Figure 12).



**Figure 12. Metrics used for each case. Desktop fingerprint sensors give us more intermediate decisions than mobile devices.**

#### 4.3.1 Molds and artefacts

As it happens with cooking, every evaluator has different abilities to generate artefacts and it is very difficult to compare one's expertise to another. Therefore, the results of the PAD evaluation are dependent on who the attacker is, as it will be shown

with evaluation results in Chapter 6. Thus, for a report, it is a good practice to include images of molds, artefacts and sample images used in the evaluation.

#### 4.4 PAD evaluation studies overview

The goal of this part of the document is to give an outline of the experiments made following this methodology and the storyline that binds them all together. In the context of presentation attack detection evaluations, the main goal was to assess the influence of different factors: different types of devices (desktop and mobile), PAI species (materials) used to create fake fingers, how many attackers tried spoofing those devices, the level of cooperation from the capture subject and the evaluator's access to the biometric system.

For that end, five different studies were performed sequentially, each with a different question in mind and as follow-ups to the previous:

- **Study 1:** how easy is it to successfully attack off-the-shelf desktop sensors with readily available materials, both with and without cooperation from the capture subject?
- **Study 2:** mobile devices with an embedded fingerprint reader are widely used nowadays, but no public PAD evaluations have been performed on them. How would the most successful cooperative PAI species from Study 1 work on mobile devices?
- **Study 3:** once cooperative attacks have been tried on mobile devices, can we have a more real-life approach and try with the non-cooperative ones? Can we find the easiest approach for stealing latent fingerprints from a phone screen?
- **Study 4:** our intuition says that different attackers would get different results, as would different chefs with the same recipe. Thus, would different attackers with the same recipe, methods and time, get the same results? Would they get similar results to those of the experimented attackers?
- **Study 5:** Having 12 hours to attack a mobile device, how many attacks will be successful, having non-experienced attackers? What new PAI species can be found?

An overview of the differences between each study and the evaluation characteristics can be seen on Figure 13, and the reader can use it as a continuous reference. The meaning of each symbol can be found at the beginning of this document, in the List of Symbols. Every study will be explained in detail throughout the next two chapters.

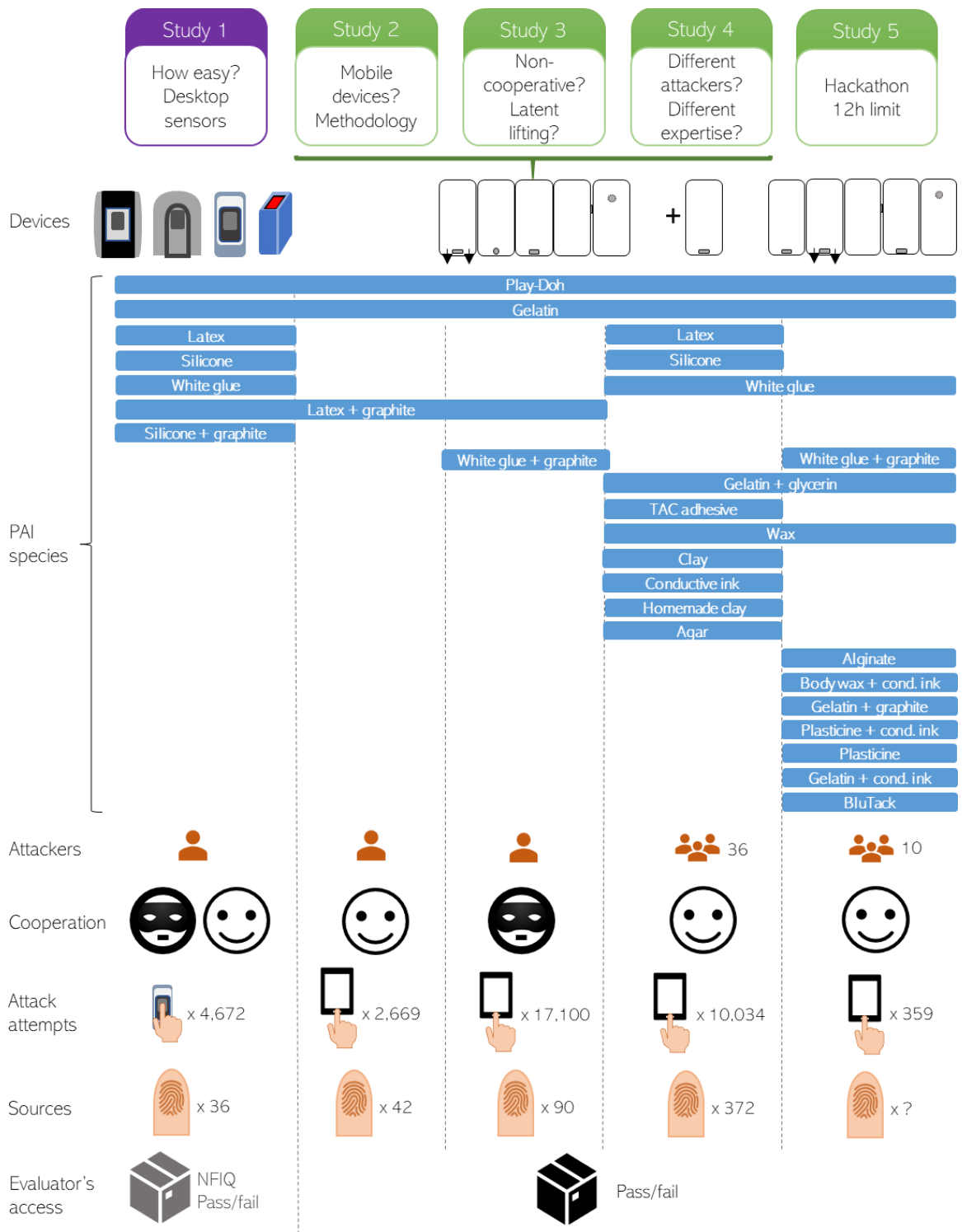


Figure 13. Overview of all carried out PAD evaluation studies.





## **Chapter 5. Presentation Attack Detection evaluation of desktop fingerprint sensors**

---

AS IT WAS seen on the studies outline of the previous section (Figure 13), Study 1 comprises an experiment made with 4 desktop fingerprint sensors of different technologies. The goal was to perform a PAD evaluation on desktop commercial readers to see their ability to reject artefacts made of several materials. In total, 4,672 attacks were attempted using 7 different PAI species (fake finger material). Both cooperative and non-cooperative tests were made, and the results were reported according to ISO/IEC 30107-3 metrics. As it was mentioned on Chapter 4, the steps for carrying out an evaluation are planning, execution and results reporting. These will be addressed throughout the subsections of this chapter. An overview of the study can be seen on Figure 14.

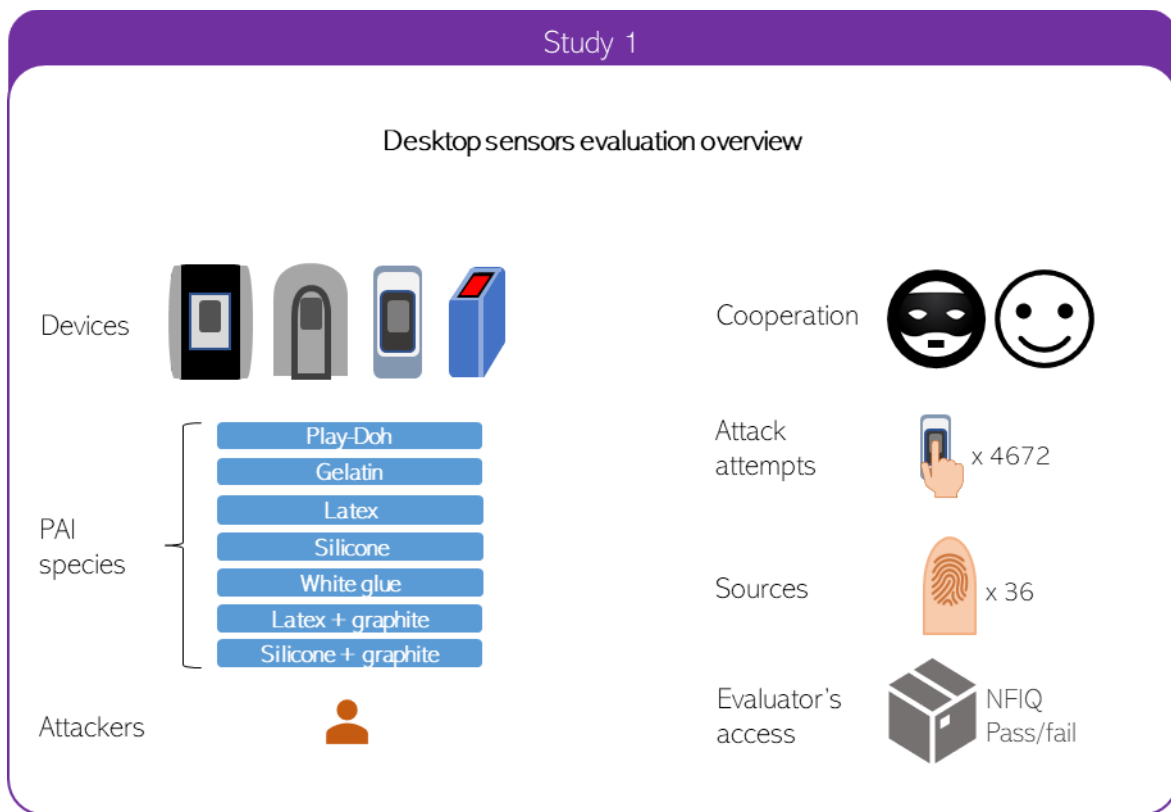


Figure 14. Overview of Study 1 characteristics.

## 5.1 Planning

As detailed on Chapter 4, the methodology used for this study (as with the rest) follows evaluation methods from Common Criteria’s CEM and ISO/IEC 30107-3. All the steps explained in the general methodology will be addressed for each study in Chapter 5 and Chapter 6.

An expert performed an evaluation on 1 thermal, 2 capacitive and 1 optical sensors. The SDKs used for the capture application did not have PAD mechanisms deactivated, that is, the configuration was the same used for performance evaluations. The process used to create the artefacts was the usual one seen in many evaluations and research on PAD [13], both cooperative (capture subject cooperates in the creation of the mold) and non-cooperative (attacker steals biometric characteristic with no help from capture subject). For this study, it was important to try many PAI species (i.e. Play-Doh, gelatin, latex, silicone, white glue, latex with graphite and silicone with graphite) to check which ones were more threatening to the systems. Details of the step “Identification of all possible threats and attacks” can be found on Table 7 and Table 8.

The enrollment and verification policies rely on quality outcomes, using the NIST Fingerprint Image Quality (NFIQ) algorithm. This measurement ranges from 1 to 5, 1 being the highest quality and 5 being the lowest. For this evaluation, samples with an NFIQ of 3 or lower get successfully acquired by the system. Consequently, samples with an NFIQ of 5 get rejected.

**Table 7. Identification of all possible threats and attacks: description of TOE.**

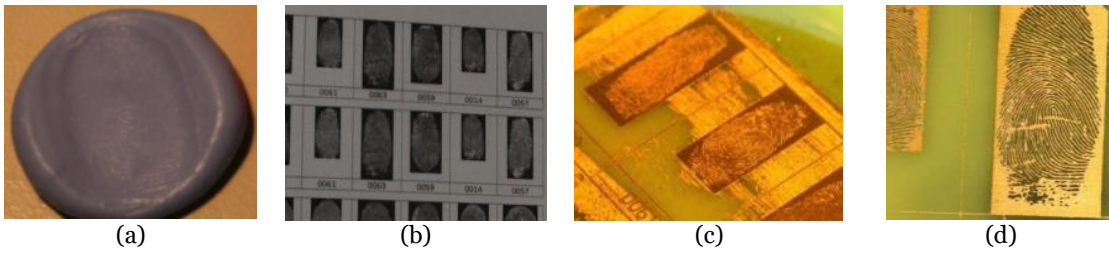
<b>Sensors</b>	<b>Thermal</b>	Resolution	385 dpi
		Image capture area	11.9 x 16.9 mm
		Fingerprint image size	180 x 256 px
	<b>Capacitive 1</b>	Resolution	363 dpi
		Image capture area	10.6 x 14 mm
		Fingerprint image size	152 x 200 px
	<b>Capacitive 2</b>	Resolution	508 dpi
		Image capture area	12.8 x 18 mm
		Fingerprint image size	256 x 360 px
	<b>Optical</b>	Resolution	508 dpi
Image capture area		12.9 x 16.8 mm	
Fingerprint image size		258 x 336 px	
<b>Evaluator's access</b>		Grey box (NFIQ quality score) Full system No PAD implemented	

**Table 8. Identification of all possible threats and attacks: description of target application.**

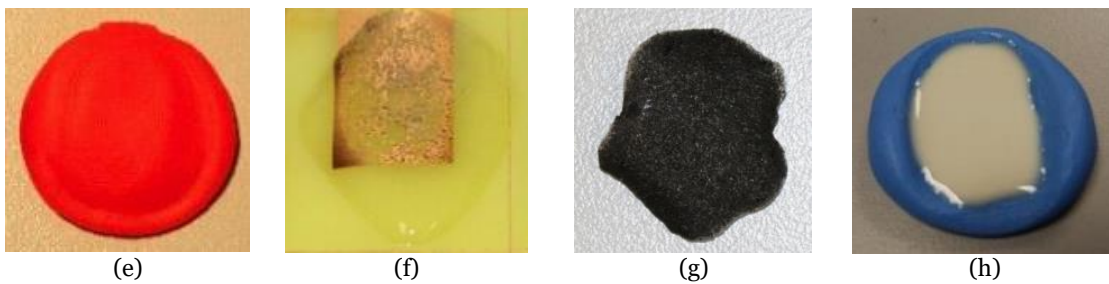
<b>Applications</b>	No particular application for this evaluation, e.g. entering an office, spending food coupons, accessing critical infrastructures, etc.
<b>Consequences of successful attack</b>	Unauthorized person entering an office, access to privileges that do not belong to person, unauthorized person fiddling with critical infrastructure.
<b>Implemented functions</b>	Enrollment: <ul style="list-style-type: none"> <li>• 2 transactions with NFIQ <math>\leq 3</math> (good quality)</li> <li>• 3 attempts per transaction until both images successfully compared (NBIS algorithm)</li> <li>• If after 3 attempts, no successful comparisons between 2 samples -&gt; no enrollment</li> <li>• Threshold for ground truth: 20 (NBIS algorithm)</li> </ul>
	Verification: <ul style="list-style-type: none"> <li>• Offline. NBIS algorithm comparison</li> <li>• 2 transactions with NFIQ <math>\leq 3</math> (good quality)</li> <li>• 3 attempts per transaction until both images successfully compared (NBIS algorithm)</li> <li>• Threshold for ground truth: 20 (NBIS algorithm)</li> </ul>

The procedure for creating the molds and artefacts has been widely reported on the literature [7], [10], [13], [45], so only a brief summary will be given here. For cooperative attacks, the capture subject presses his or her finger on a silicone ball for around 5 minutes, until it hardens. That will be the mold. To create the artefact, materials are pressed or spread across the mold for a given time. For non-cooperative attacks, the capture subject leaves a trace of his or her fingerprint on a surface. The shape is enhanced by brushing ink powder on it, and a high-quality photo is taken. This picture is digitally enhanced with freely available software and printed on a transparent sheet. This sheet will then be laid on a PCB (printed circuit board) that can be

developed to obtain a 3D mold. Lastly, the same steps as with the cooperative attacks are followed to build an artefact. Some steps can be seen on Figure 15 and Figure 16.



**Figure 15. Process for obtaining molds: a) Cooperative silicon mold after having a pressed finger, b) fingerprints printed on transparent sheet, c) PCB board being developed and d) resulting non-cooperative PCB mold.**



**Figure 16. Resulting artefacts: e) Play-Doh artefact, f) gelatin artefact on a non-cooperative mold, g) latex with graphite artefact and h) latex artefact on a cooperative mold during the drying process.**

### 5.1.1 Analysis of Attack Potential

As it was explained on Chapter 4 Section 4.1.2 *Analysis of Attack Potential*, the attack potential is a measure of the effort to be expended in attacking a TOE with a PAI, expressed in terms of an attacker’s expertise, resources and motivation, which can be divided into more specific parameters. In this way, TOEs are given a rating to assess their resistance to specific attacks. As explained previously, every threat has a corresponding attack. The particular case for this study can be seen on Table 9.

**Table 9. Planning: Analysis of attack potential by searching threats and their corresponding attacks (study on desktop sensors).**

<p><b>Possible threats</b></p>	<ul style="list-style-type: none"> <li>• Only presentation attack: using an artefact generated from a user’s real finger on the reader.</li> <li>• Intended operation of the system: depends on the target application, e.g. opening a door to an office or to a gym or getting privileges like food coupons.</li> </ul>
<p><b>Possible attacks</b></p>	<ul style="list-style-type: none"> <li>• Corresponding attack: presentation attack.</li> <li>• Biometric characteristic can be obtained with or without cooperation from the capture subject. In this case, both were done.</li> <li>• Level of expertise of the evaluator: proficient, although the materials needed for the evaluation can be found at any supermarket.</li> </ul>

### 5.1.1.1 Attack Potential calculation

This calculation is used by the evaluator to determine whether or not the TOE is resistant to attacks assuming a specific attack potential of an attacker [18]. If the evaluator determines that a potential vulnerability is exploitable in the fingerprint sensor, they must confirm that it is exploitable by doing penetration tests (as specified on Section 4.1.2).

With this in mind, the evaluator determines the minimum attack potential required by an attacker to successfully carry on an attack and arrives at some conclusion about the TOE's resistance to attacks. This attack potential is confirmed on the penetration tests performed in this work on subsection 5.1.2.

As explained on Chapter 4, a score can be assigned to each of the attack potential parameters. By adding all the values, the attack potential of an PAI species is rated as Basic, Enhanced-Basic, Moderate, High or Beyond high.

Following CEM specifications, a score was given to every parameter of the attack potential to calculate its total rating (each score is given according to the table on [18]). The attack potential will be different for cooperative and non-cooperative attacks, being the expertise and the elapsed time the most differentiating factors, as can be seen on Table 10 and Table 11. As all the materials used for this experiment were readily available and easy to use, all of them sum up the same attack potential score.

**Table 10. Attack Potential calculation for cooperative attacks on desktop fingerprint sensors. Scores assigned according to the classification from Common Criteria [18, p. 429].**

COOPERATIVE ATTACKS					
	Preparation phase	PAI construction + exercising phase	Attack execution phase	Total factor rating	Score
Elapsed time	<1 day (capture subject is cooperative)	<1 day or <1 week (different material difficulty)	Few seconds (perform attack)	<1 week or <2 weeks	1.5
Expertise	Layman (information about effective materials is widely available on the internet)	Layman (easy to create)	Layman (not much expertise needed)	Layman	0
Knowledge of TOE	Public (well known on the internet that it works)	Public (manuals can be found on the internet)	Public (no knowledge needed)	Public	0
Window of opportunity	Unnecessary (no access to TOE needed)	Easy (access to TOE for practicing)	Depends on scenario	Easy	1
Equipment	Standard (materials easy to obtain in supermarkets or online)	Specialized (some sensors might be hard to obtain for practicing)	Standard (no equipment needed)	Specialized	4
<b>Overall attack rating</b>	<b>6.5 (Basic)</b>				
<b>Attack resistance</b>	<b>Minimum</b>				

**Table 11. Attack Potential calculation for non-cooperative attacks on desktop fingerprint sensors. Scores assigned according to the classification from Common Criteria [18, p. 429].**

NON-COOPERATIVE ATTACKS					
	Preparation phase	PAI construction + exercising phase	Attack execution phase	Total factor rating	Score
Elapsed time	<1 week (capture subject is non-cooperative)	1 week (creating PAIs)	Few seconds (perform attack)	<2 weeks	2
Expertise	Layman (information about effective materials is widely available on the internet)	Proficient (process needs many steps)	Layman (not much expertise needed)	Proficient	3
Knowledge of TOE	Public (well known on the internet that it works)	Public (manuals can be found on the internet)	Public (no knowledge needed)	Public	0
Window of opportunity	Unnecessary (no access to TOE needed)	Easy (access to TOE for practicing)	Depends on scenario	Easy	1
Equipment	Standard (materials easy to obtain in supermarkets or online, but it takes time to learn the procedure)	Specialized (some sensors might be hard to obtain)	Standard (no equipment needed)	Specialized	4
<b>Overall attack rating</b>	<b>10 (Enhanced-basic)</b>				
<b>Attack resistance</b>	<b>Basic</b>				

As it was calculated on Table 10 and Table 11, the rating for cooperative attacks on desktop fingerprint readers is 6.5 (basic) and 10 (enhanced-basic) for the non-cooperative. Thus, the attacks would have to be considered in penetration testing for all evaluations assuming, respectively, Minimum and Basic attack potentials (or higher). If penetration tests show that the attack is successful, the TOE would fail to resist against that attack potential.

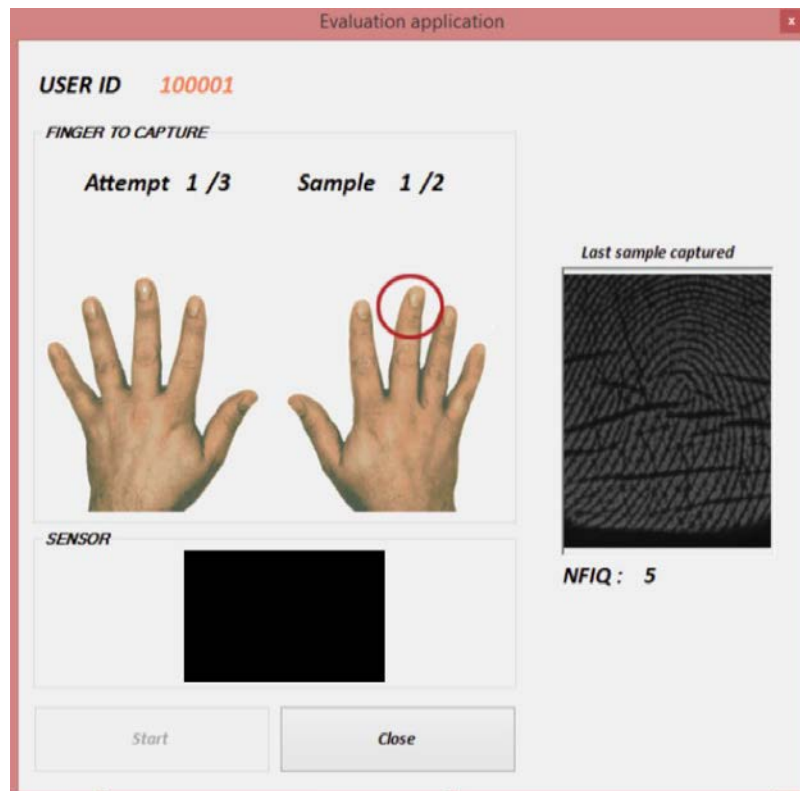
### 5.1.2 Specification of penetration test

Once the TOE has been analyzed and described, the penetration test can be planned. A comparison with the rest of the studies was given in Section 4.4, if context is wanted.

**Table 12. Penetration test characteristics for the study on desktop sensors.**

	<b>Cooperative attacks</b>	<b>Non cooperative attacks</b>
<b>Sensors</b>	1 thermal, 2 capacitive, 1 optical	1 thermal, 2 capacitive
<b>Capture subjects</b>	6 (4 male, 2 female)	
<b>Sources per capture subject (fingers)</b>	6 (index, middle and thumb from both hands)	
<b>Total sources (fingers)</b>	36 (not all sources used for all PAI species)	
<b>Attempts per finger</b>	3	
<b>Total attempts</b>	2,520	2,668
<b>Sessions</b>	2 for bona fide (15 days apart), 1 for attacks	
<b>PAI species</b>	7 (Silicone, silicone + graphite, gelatin, latex, latex + graphite, Play-Doh, white glue)	
<b>Molds</b>	Silicone	
<b>Evaluator's access</b>	Grey box (NFIQ quality score, pass/fail result)	
<b>Evaluator number and expertise</b>	1 expert	

For the data collection, an app was developed for the capture process. As it can be seen on Figure 17, the program showed which finger to capture, the number of attempts and samples left and an image of the captured fingerprint. It allowed both an enrollment and verification process.



**Figure 17. Example display of the desktop capture program.**

## 5.2 Execution

As it was explained on Section 4.2, the execution can be done once the penetration test has been specified. It comprises three phases: detection, capture and processing.

### 5.2.1 Detection

Before the actual execution, the different PAI species were put to the test. If the sensor could detect the fingerprint, then it could be selected for the evaluation.

### 5.2.2 Capture

As checking the quality is not always possible for the evaluator, some artefacts with different qualities (examined by the evaluator) can be used to check which ones are obtained successfully by the sensor, and continue with that technique [93]. For desktop capture devices, the quality of the sample could be measured with NFIQ and an image of the sample could be seen at the moment of capture. Thus, it was possible for the evaluator to improve the attack during the evaluation. It also must be noted that different artefacts work better on sensors with different technologies: transparent PAIs, in general, do not work well on optical sensors because of the light scattering; non-conductive PAIs do not work on capacitive sensors.

It was observed that, depending on the environmental conditions, some materials behave differently. In hot weather (25 degrees Celsius or more), Play-Doh and gelatin artefacts are very difficult to use, as they lose their shape in seconds, sometimes before reaching the reader. On the other hand, latex becomes softer and more moist, so it becomes conductive and is thus detected by capacitive sensors.

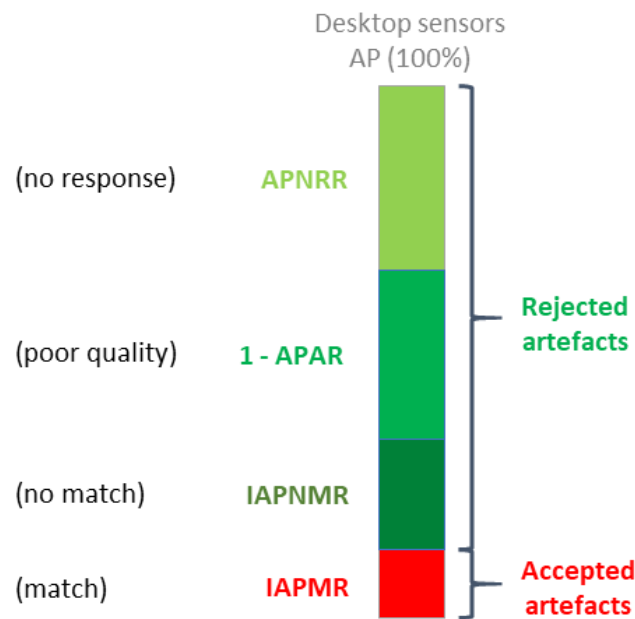
### 5.2.3 Processing

In the case of desktop fingerprint capture devices, all images were stored for an offline verification with the database of subjects' real fingers by using the NBIS algorithm by NIST [94]. The most significant values from the analysis were the proportion of times that an artefact was verified as a bona fide presentation and the proportion of images that were rejected by the system due to low quality (NFIQ > 4).

## 5.3 Results

After the penetration test is executed, the results from the PAD evaluation can be obtained and analyzed. As it was explained on Section 4.3.2, the metrics that can be reported for this study are APNRR, APAR and IAPMR (Figure 18). This is valid for all sensors.





**Figure 18. Results reporting metrics, according to ISO/IEC 30107-3. This applies to all sensors.**

As having successful PAIs is an undesirable outcome, the number of successful attacks will be represented in red, while unsuccessful attacks will be shown in green in all graphs.

### 5.3.1 Penetration test results

This subsection is divided into cooperative and non-cooperative attacks. While cooperative attacks were performed on all readers (one thermal, two capacitive and one optical), for the case of non-cooperative attacks the optical was not used. This is due to having carried out two separate studies and adding the optical sensor only on the second one, where only cooperative attacks were done.

#### 5.3.1.1 Cooperative attacks

As explained on previous sections, cooperative attacks require the collaboration of the capture subject to obtain his or her fingerprints. This is done by laying his or her finger on a material for a specific amount of time until the shape is transferred to the mold. Thus, in general, samples obtained in this manner should attain a higher quality. For this reason, an image quality analysis will be shown, measured with NIST Fingerprint Image Quality (NFIQ). The policy for verification based on NFIQ was covered on subsection 5.1. The quality analysis for each PAI species and device, along with sample images obtain for each case, are shown on Table 13 -Table 19. In those cases where there is no image, it means that the sensor could not detect the artefact or acquire any sample. Moreover, not all samples shown on the table resulted in a successful acquirement, as many of them obtained an NFIQ of 5.

**Table 13. NFIQ distribution by sensor for cooperative attacks, for the case of gelatin.**

Material	NFIQ distribution	Sensor																										
Gelatin	<table border="1"> <caption>NFIQ Distribution for Gelatin</caption> <thead> <tr> <th>NFIQ Level</th> <th>Ther</th> <th>Cap1</th> <th>Cap2</th> <th>Opt</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>~20</td> <td>~10</td> <td>0</td> <td>0</td> </tr> <tr> <td>2</td> <td>~10</td> <td>~10</td> <td>~10</td> <td>~10</td> </tr> <tr> <td>3</td> <td>~40</td> <td>~30</td> <td>~40</td> <td>~10</td> </tr> <tr> <td>5</td> <td>~100</td> <td>~240</td> <td>~60</td> <td>~10</td> </tr> </tbody> </table>	NFIQ Level	Ther	Cap1	Cap2	Opt	1	~20	~10	0	0	2	~10	~10	~10	~10	3	~40	~30	~40	~10	5	~100	~240	~60	~10	<b>Thermal</b> 	<b>Capacitive 1</b> 
		NFIQ Level	Ther	Cap1	Cap2	Opt																						
1	~20	~10	0	0																								
2	~10	~10	~10	~10																								
3	~40	~30	~40	~10																								
5	~100	~240	~60	~10																								
<b>Capacitive 2</b> 	<b>Optical</b> 																											

**Table 14. NFIQ distribution by sensor for cooperative attacks, for the case of Play-Doh.**

Material	NFIQ distribution	Sensor																										
Play-Doh	<table border="1"> <caption>NFIQ Distribution for Play-Doh</caption> <thead> <tr> <th>NFIQ Level</th> <th>Ther</th> <th>Cap1</th> <th>Cap2</th> <th>Opt</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>~20</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>2</td> <td>~10</td> <td>~10</td> <td>~10</td> <td>~10</td> </tr> <tr> <td>3</td> <td>~80</td> <td>~20</td> <td>~20</td> <td>~10</td> </tr> <tr> <td>5</td> <td>~90</td> <td>~360</td> <td>~150</td> <td>~10</td> </tr> </tbody> </table>	NFIQ Level	Ther	Cap1	Cap2	Opt	1	~20	0	0	0	2	~10	~10	~10	~10	3	~80	~20	~20	~10	5	~90	~360	~150	~10	<b>Thermal</b> 	<b>Capacitive 1</b> 
		NFIQ Level	Ther	Cap1	Cap2	Opt																						
1	~20	0	0	0																								
2	~10	~10	~10	~10																								
3	~80	~20	~20	~10																								
5	~90	~360	~150	~10																								
<b>Capacitive 2</b> 	<b>Optical</b> 																											

**Table 15. NFIQ distribution by sensor for cooperative attacks, for the case of latex.**

Material	NFIQ distribution	Sensor																										
Latex	<table border="1"> <caption>NFIQ Distribution for Latex</caption> <thead> <tr> <th>NFIQ Level</th> <th>Ther</th> <th>Cap1</th> <th>Cap2</th> <th>Opt</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>~10</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>2</td> <td>~20</td> <td>~10</td> <td>~10</td> <td>~10</td> </tr> <tr> <td>3</td> <td>~40</td> <td>~10</td> <td>~10</td> <td>~10</td> </tr> <tr> <td>5</td> <td>~40</td> <td>~230</td> <td>0</td> <td>0</td> </tr> </tbody> </table>	NFIQ Level	Ther	Cap1	Cap2	Opt	1	~10	0	0	0	2	~20	~10	~10	~10	3	~40	~10	~10	~10	5	~40	~230	0	0	<b>Thermal</b> 	<b>Capacitive 1</b> 
		NFIQ Level	Ther	Cap1	Cap2	Opt																						
1	~10	0	0	0																								
2	~20	~10	~10	~10																								
3	~40	~10	~10	~10																								
5	~40	~230	0	0																								
<b>Capacitive 2</b> -	<b>Optical</b> 																											

**Table 16. NFIQ distribution by sensor for coop. attacks, for the case of latex+graphite.**

Material	NFIQ distribution	Sensor																										
Latex with graphite	<table border="1"> <caption>NFIQ Distribution Data for Latex with graphite</caption> <thead> <tr> <th>NFIQ Level</th> <th>Ther</th> <th>Cap1</th> <th>Cap2</th> <th>Opt</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>2</td> <td>10</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>3</td> <td>40</td> <td>10</td> <td>0</td> <td>0</td> </tr> <tr> <td>5</td> <td>100</td> <td>320</td> <td>0</td> <td>0</td> </tr> </tbody> </table>	NFIQ Level	Ther	Cap1	Cap2	Opt	1	0	0	0	0	2	10	0	0	0	3	40	10	0	0	5	100	320	0	0	<b>Thermal</b> 	<b>Capacitive 1</b> 
		NFIQ Level	Ther	Cap1	Cap2	Opt																						
1	0	0	0	0																								
2	10	0	0	0																								
3	40	10	0	0																								
5	100	320	0	0																								
<b>Capacitive 2</b> 	<b>Optical</b> 																											

**Table 17. NFIQ distribution by sensor for cooperative attacks, for the case of silicone.**

Material	NFIQ distribution	Sensor																										
Silicone	<table border="1"> <caption>NFIQ Distribution Data for Silicone</caption> <thead> <tr> <th>NFIQ Level</th> <th>Ther</th> <th>Cap1</th> <th>Cap2</th> <th>Opt</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>2</td> <td>0</td> <td>0</td> <td>0</td> <td>5</td> </tr> <tr> <td>3</td> <td>15</td> <td>5</td> <td>0</td> <td>0</td> </tr> <tr> <td>5</td> <td>40</td> <td>60</td> <td>0</td> <td>0</td> </tr> </tbody> </table>	NFIQ Level	Ther	Cap1	Cap2	Opt	1	0	0	0	0	2	0	0	0	5	3	15	5	0	0	5	40	60	0	0	<b>Thermal</b> 	<b>Capacitive 1</b> 
		NFIQ Level	Ther	Cap1	Cap2	Opt																						
1	0	0	0	0																								
2	0	0	0	5																								
3	15	5	0	0																								
5	40	60	0	0																								
<b>Capacitive 2</b> -	<b>Optical</b> 																											

**Table 18. NFIQ distribution by sensor for cooperative attacks, for the case of silicone with graphite.**

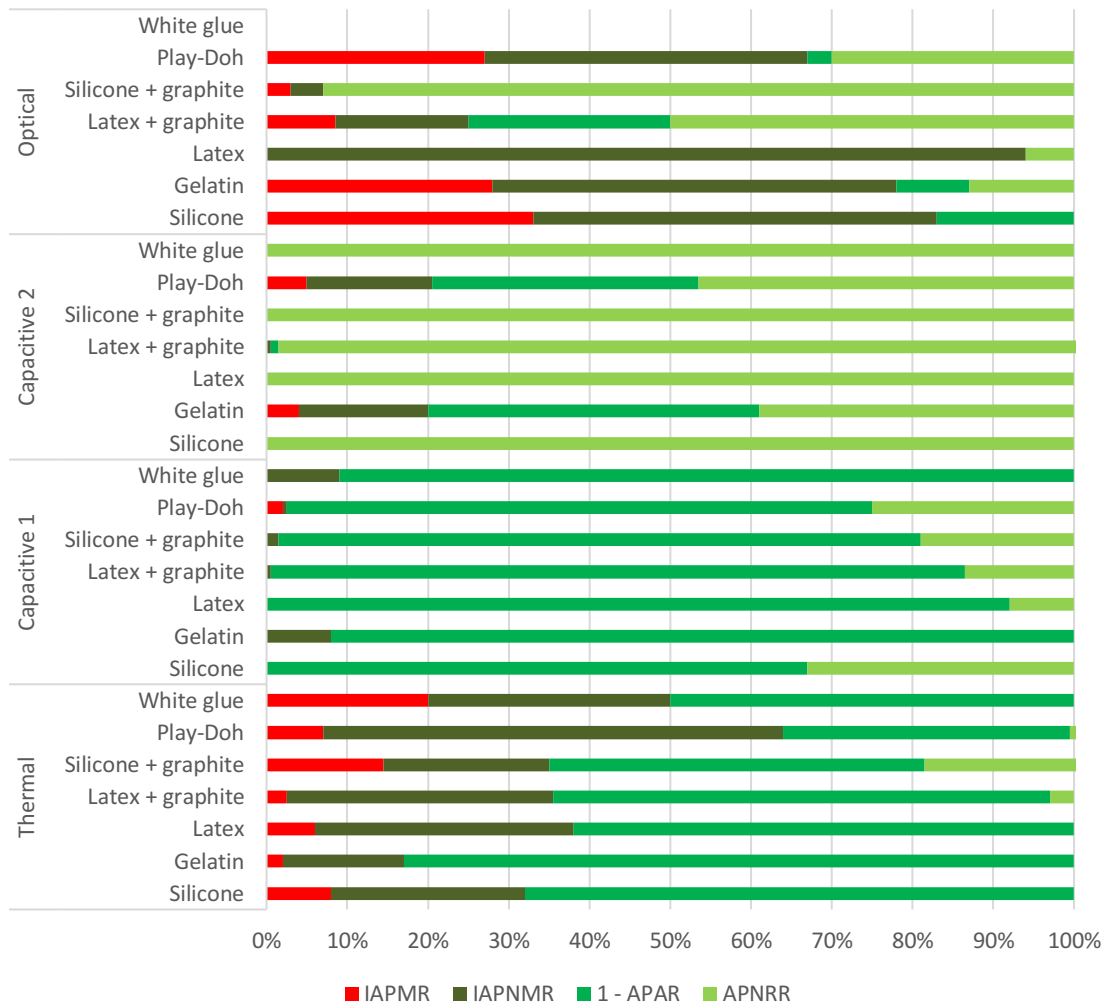
Material	NFIQ distribution	Sensor																										
Silicone with graphite	<table border="1"> <caption>NFIQ Distribution Data for Silicone with graphite</caption> <thead> <tr> <th>NFIQ Level</th> <th>Ther</th> <th>Cap1</th> <th>Cap2</th> <th>Opt</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>2</td> <td>10</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>3</td> <td>20</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>5</td> <td>30</td> <td>130</td> <td>0</td> <td>0</td> </tr> </tbody> </table>	NFIQ Level	Ther	Cap1	Cap2	Opt	1	0	0	0	0	2	10	0	0	0	3	20	0	0	0	5	30	130	0	0	<b>Thermal</b> 	<b>Capacitive 1</b> 
		NFIQ Level	Ther	Cap1	Cap2	Opt																						
1	0	0	0	0																								
2	10	0	0	0																								
3	20	0	0	0																								
5	30	130	0	0																								
<b>Capacitive 2</b> -	<b>Optical</b> 																											

**Table 19. NFIQ distribution by sensor for cooperative attacks, for the case of white glue.**

Material	NFIQ distribution	Sensor																										
		Thermal	Capacitive 1																									
White glue	<table border="1"> <caption>NFIQ Distribution Data for White Glue</caption> <thead> <tr> <th>NFIQ Score</th> <th>Ther (Blue)</th> <th>Cap1 (Red)</th> <th>Cap2 (Green)</th> <th>Opt (Purple)</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0</td> <td>3</td> <td>0</td> <td>0</td> </tr> <tr> <td>2</td> <td>2</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>3</td> <td>7</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>5</td> <td>10</td> <td>30</td> <td>0</td> <td>0</td> </tr> </tbody> </table>	NFIQ Score	Ther (Blue)	Cap1 (Red)	Cap2 (Green)	Opt (Purple)	1	0	3	0	0	2	2	0	0	0	3	7	0	0	0	5	10	30	0	0		
		NFIQ Score	Ther (Blue)	Cap1 (Red)	Cap2 (Green)	Opt (Purple)																						
1	0	3	0	0																								
2	2	0	0	0																								
3	7	0	0	0																								
5	10	30	0	0																								
		Capacitive 2 -																										

As it can be clearly seen, most artefacts obtain an NFIQ score of 5, which is the lowest quality. The thermal sensor is more widely distributed, having most artefacts divided in NFIQ 3 and 5, but also many with NFIQ 1 and 2. For capacitive reader 1, many images are only a completely black sample, which NFIQ considers has a score of 5. Latex is the material which provides the best quality, but only for the thermal and optical devices. Gelatin and Play-Doh are the ones that obtain the best quality on capacitive sensors, and they are the only materials that produce a detectable sample on all 4 readers.

As it was seen on Figure 18, the results report according to ISO/IEC 30107-3 must include IAPMR, APAR and IAPNRR. The results for the cooperative experiments can be seen on Figure 19.



**Figure 19. IAPMR, IAPNMR, 1-APAR and APNRR for each PAI species and each device, for the case of cooperative attacks.**

The IAPMR values expose that the only material that can successfully attack all systems is Play-Doh, especially for the case of the optical sensor. The highest IAPMRs were obtained with silicone mixed with graphite, Play-Doh and white glue. Nevertheless, it should be noted that in the case of some PAI species, the number of generated artefacts is too small compared to others. This is because, according to ISO/IEC 30107, if a material is more easily detected by readers or it succeeds more times in being compared with the reference, a bigger number of artefacts of this kind should be created. The number of fake fingers created for each PAI species can be seen on Table 20. According to ISO/IEC 30107, if a PAI species is more easily detected by the sensors, a bigger number should be created with this technique.

**Table 20. Number of artefacts built with each material for the case of cooperative attacks.**

Gelatin	Play-Doh	Latex	Latex with graphite	Silicone	Silicone with graphite	White glue
36	42	12	48	6	24	6

In addition, the greater the APNRR, the better the system is at rejecting fake samples (by not responding when they are placed on the sensor), so in this matter, the thermal reader responds to the highest number of artefacts, although as stated below, those captured samples ended up not being successful. Systems can also reject artefacts due to their low quality (NFIQ higher than 3), and this ability is represented by APAR. In this case, the capacitive sensors were more capable of rejecting non-conductive samples, even when breathing on them to create a conductive layer on the surface. Nevertheless, most of the few samples that passed the quality check for these devices were verified as a real finger and, while for the case of the thermal one, the proportion was much smaller.

5.3.1.2 Non-cooperative attacks

As explained previously, non-cooperative attacks do not require the collaboration of the capture subject to obtain his or her fingerprints. This is done by lifting a latent fingerprint left behind by the capture subject and creating a 3D mold by developing a PCB with the biometric characteristics. Thus, in general, samples obtained in this manner should attain a lower quality than with cooperative attacks. For this reason, an image quality analysis will be shown, measured with NIST Fingerprint Image Quality (NFIQ). This measurement ranges from 1 to 5, 1 being the highest quality and 5 being the lowest. As it was detailed previously, samples with an NFIQ of 3 or lower get successfully acquired by the system. Consequently, samples with an NFIQ of 5 get rejected. The quality analysis for each PAI species and sensor, along with sample images obtain for each case, are shown on Table 21 -Table 27. In those cases where there is no image, it means that the reader could not detect the artefact or acquire any sample. Moreover, not all samples shown on the table resulted in a successful acquirement, as many of them obtained an NFIQ of 5.

Table 21. NFIQ distribution by sensor for non-cooperative attacks, for the case of gelatin.

Material	NFIQ distribution	Sensor	
		Thermal	Capacitive 1
Gelatin			
			-

**Table 22. NFIQ distribution by sensor for non-coop. attacks, for the case of Play-Doh.**

Material	NFIQ distribution	Sensor	
Play-Doh	<p>Play-Doh</p> <p>■ Ther ■ Cap1 ■ Cap2</p>	<b>Thermal</b> 	<b>Capacitive 1</b> 
		<b>Capacitive 2</b> -	<b>Optical</b> -

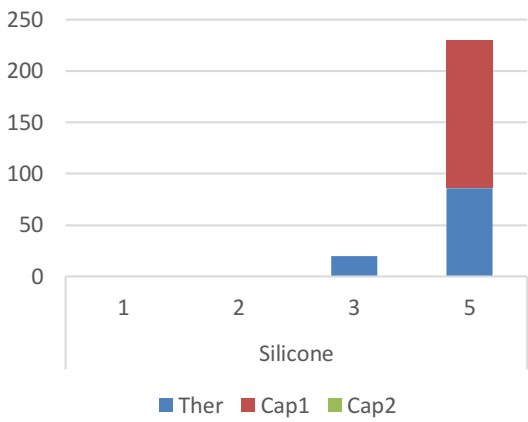

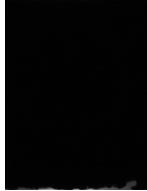
**Table 23. NFIQ distribution by sensor for non-cooperative attacks, for the case of latex.**

Material	NFIQ distribution	Sensor	
Latex	<p>Latex</p> <p>■ Ther ■ Cap1 ■ Cap2</p>	<b>Thermal</b> 	<b>Capacitive 1</b> 
		<b>Capacitive 2</b> -	<b>Optical</b> -

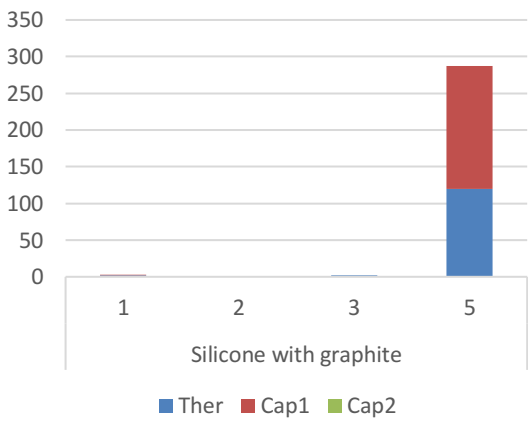

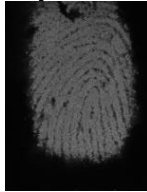
**Table 24. NFIQ distribution divided by sensor for non-coop. attacks, for latex+ graphite.**

Material	NFIQ distribution	Sensor	
Latex with graphite	<p>Latex with graphite</p> <p>■ Ther ■ Cap1 ■ Cap2</p>	<b>Thermal</b> -	<b>Capacitive 1</b> 
		<b>Capacitive 2</b> -	<b>Optical</b>

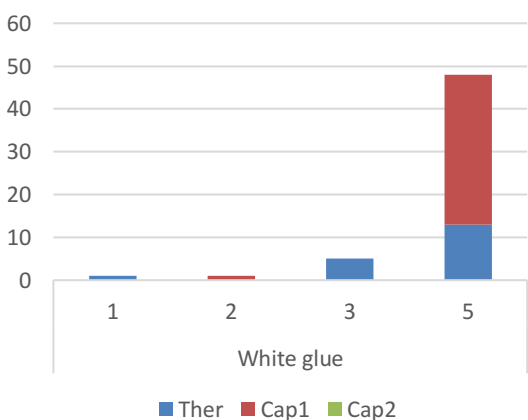

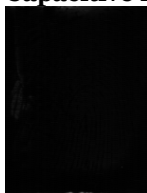
**Table 25. NFIQ distribution by sensor for non-coop. attacks, for the case of silicone.**

Material	NFIQ distribution	Sensor	
		Thermal	Capacitive 1
Silicone			
		Capacitive 2 -	Optical -

**Table 26. NFIQ distribution by sensor for non-coop. attacks, for silicone with graphite.**

Material	NFIQ distribution	Sensor	
		Thermal	Capacitive 1
Silicone with graphite			
		Capacitive 2 -	Optical -

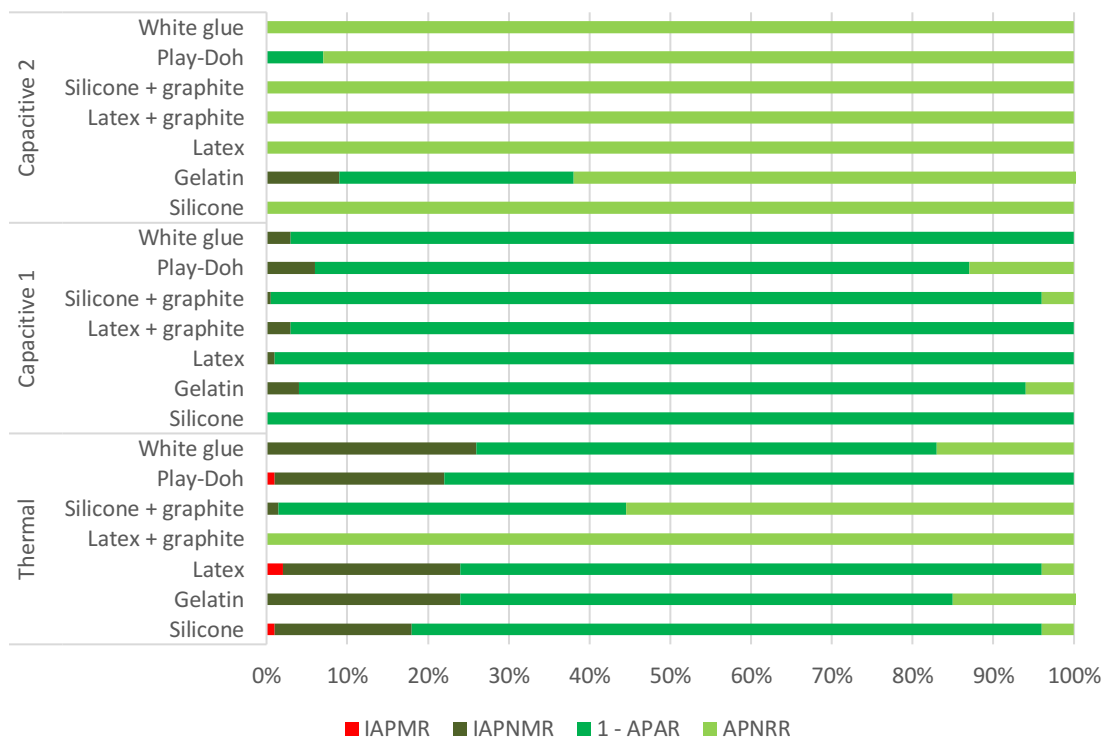
**Table 27. NFIQ distribution by sensor for non-coop. attacks, for the case of white glue.**

Material	NFIQ distribution	Sensor	
		Thermal	Capacitive 1
White glue			
		Capacitive 2 -	Optical -



As it can be seen, most artefacts fall on an NFIQ score of 5, that is, the lowest quality of the range. The only material that could be detected by capacitive reader 2 is gelatin, and in the few cases that an image could be obtained, it had an NFIQ of 5. Again, the thermal sensor can consistently acquire samples of all the materials, minus latex with graphite.

As it was seen on Figure 18, the results report according to ISO/IEC 30107-3 must include IAPMR, APAR and IAPNRR. The results for the non-cooperative experiments can be seen on Figure 20.



**Figure 20. IAPMR, IAPNMR, 1-APAR and APNRR for each PAI species and each device, for the case of non-cooperative attacks.**

As it can be observed, non-cooperative attacks were only successful on the thermal reader. On capacitive sensor 1, most artefacts were rejected due to quality (high 1 – APAR), while on capacitive sensor 2 they were rejected because they were not detected at all (no image was produced).

It must be noted that in PAD evaluations described on Chapter 3, non-collaborative attacks were done for one finger at a time. That means that for each sample, around 10 fake finger molds were produced. Then, the best mold of all was chosen for the attack. In the case of an attacker, usually only one finger is needed to enter a system, so he or she could focus on only creating one good mold of one finger. In the case of this study, 6 different fingers were done on each PCB, so from each batch only 1-2 molds were of enough quality to create fingers, giving poor attack results. The number of artefacts for each PAI species can be seen on Table 28. According to ISO/IEC 30107, if an PAI species is more easily detected by the sensors, a bigger number should be created with this technique.

**Table 28. Number of artefacts built with each material for the case of non-cooperative attacks.**

Gelatin	Play-Doh	Latex	Latex with graphite	Silicone	Silicone with graphite	White glue
30	18	24	12	24	30	6

### 5.3.2 Vulnerability test results

As it was explained on Section 4.3.1, once all the data has been analyzed after the penetration test, the evaluator shall report which PAI species were successful in attacking each system to report their found vulnerabilities to presentation attacks. It must be noted that some PAI species were used more times than others. The result for these experiments is shown on Table 29.

**Table 29. List of vulnerabilities of desktop sensors. It must be noted that not all PAI species were tried on every reader and that different numbers of attempts were performed on each experiment.**

PAI species	Thermal	Capacitive 1	Capacitive 2	Optical
Silicone	x			x
Gelatin	x		x	x
Latex	x			
Latex + graphite	x			x
Silicone + graphite	x			x
Play-Doh	x	x	x	x
White glue	x			

The consequences that may derive from these vulnerabilities are several, because these kinds of readers can be used for many applications. For example, an unintended user could access a gym or office or, in more critical circumstances, bypass a frontier or a critical infrastructure.

## 5.4 Conclusions

The goal of this work was to analyze the possible vulnerabilities of desktop fingerprint sensors, focusing on attacks that do not need lots of expertise, performed with cheap materials that are readily available at supermarkets or online marketplaces. Moreover, at the time the work was developed, the standard ISO/IEC 30107-3 *Presentation Attack Detection evaluation* was at its early stages and no evaluations had been performed following the last version of the document. As a consequence, contributions were done to the standard with the experience gained during this experiment.

Although some conclusions could be obtained from the studies, a bigger database would be needed for some specific materials. This work was made only to get an outline of the possible vulnerabilities of fingerprint systems by trying 7 combinations of materials: silicone, gelatin, latex, latex with graphite, silicone with graphite, Play-Doh

and white glue. A system is considered to be breached security-wise when one single attack is successful, and all sensors were spoofed at least once.

In the literature analysis of PAD evaluations described on Chapter 3, non-collaborative attacks were done for one finger at a time. That means that for each sample, around 10 fake finger molds were produced. Then, the best mold of all was chosen for the attack. In the case of an attacker, usually only one finger is needed to enter a system, so he or she could focus on only creating one good mold of one finger. In the case of this study, 6 different fingers were done on each PCB, so from each batch only 1-2 molds were of enough quality to create fingers. Thus, results could be better if each finger mold was done repeatedly until obtaining a decent mold.

Some materials were harmful for capture devices. White glue, for instance, was too harsh to be placed on the sensor. Silicone obtained good spoofing results when a lot of pressure was put on the reader, but if a normal force was applied, the PAD error rates dropped to zero.

As it was mentioned, this study was performed in two periods, winter and summer, and some materials appeared to be highly influenced by this fact. Latex becomes sticky and wet with heat, so it is more effective spoofing capacitive sensors, as they are based on conductivity, so it is more effective in a warm environment. Play-Doh deforms easily with heat and traces get erased, while cold environments allow it to keep its shape, thus being more effective in a cold environment.

## 5.5 Contributions and dissemination

This study was published as a conference paper and as part of a journal paper. Also, it was part of the Master Thesis written by the author.

### 5.5.1 Journal papers

[95] I. Goicoechea-Telleria, R. Sanchez-Reillo, J. Liu-Jimenez, and R. Blanco-Gonzalo, “Attack Potential Evaluation in Desktop and Smartphone Fingerprint Sensors: Can They Be Attacked by Anyone?,” *Hindawi*, vol. 2018, pp. 1–13, 2018.

### 5.5.2 Conference papers

[23] I. Goicoechea-Telleria, B. Fernandez-Saavedra, and R. Sanchez-Reillo, “An Evaluation of Presentation Attack Detection of Fingerprint Biometric Systems applying ISO / IEC 30107-3,” in *International Biometric Performance Testing Conference*, 2016.

### 5.5.3 Standardization

[1] ISO / IECJTC 1 / SC37, “Text of FDIS 30107-3, Information technology — Biometric presentation attack detection — Part 3: Testing and reporting,” *ISO-IEC Standards*, vol. 2008. 2009.

- Contributed to the standard by clarifying concepts and adding new ones.

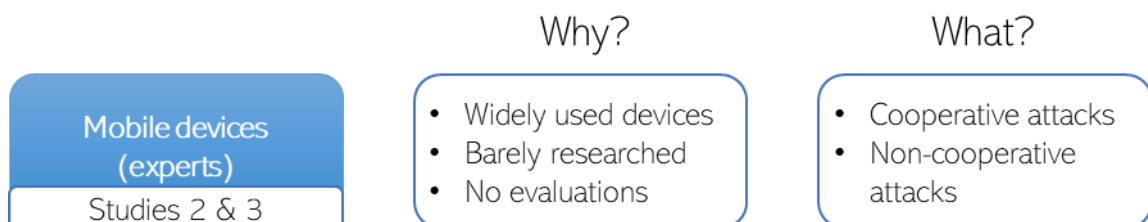
#### 5.5.4 Others

[96] I. Goicoechea-Telleria, "Vulnerabilities in Fingerprint Biometric Recognition," Master Thesis, Carlos III University of Madrid, 2015.

## Chapter 6. Presentation Attack Detection evaluation of mobile devices - single experts

---

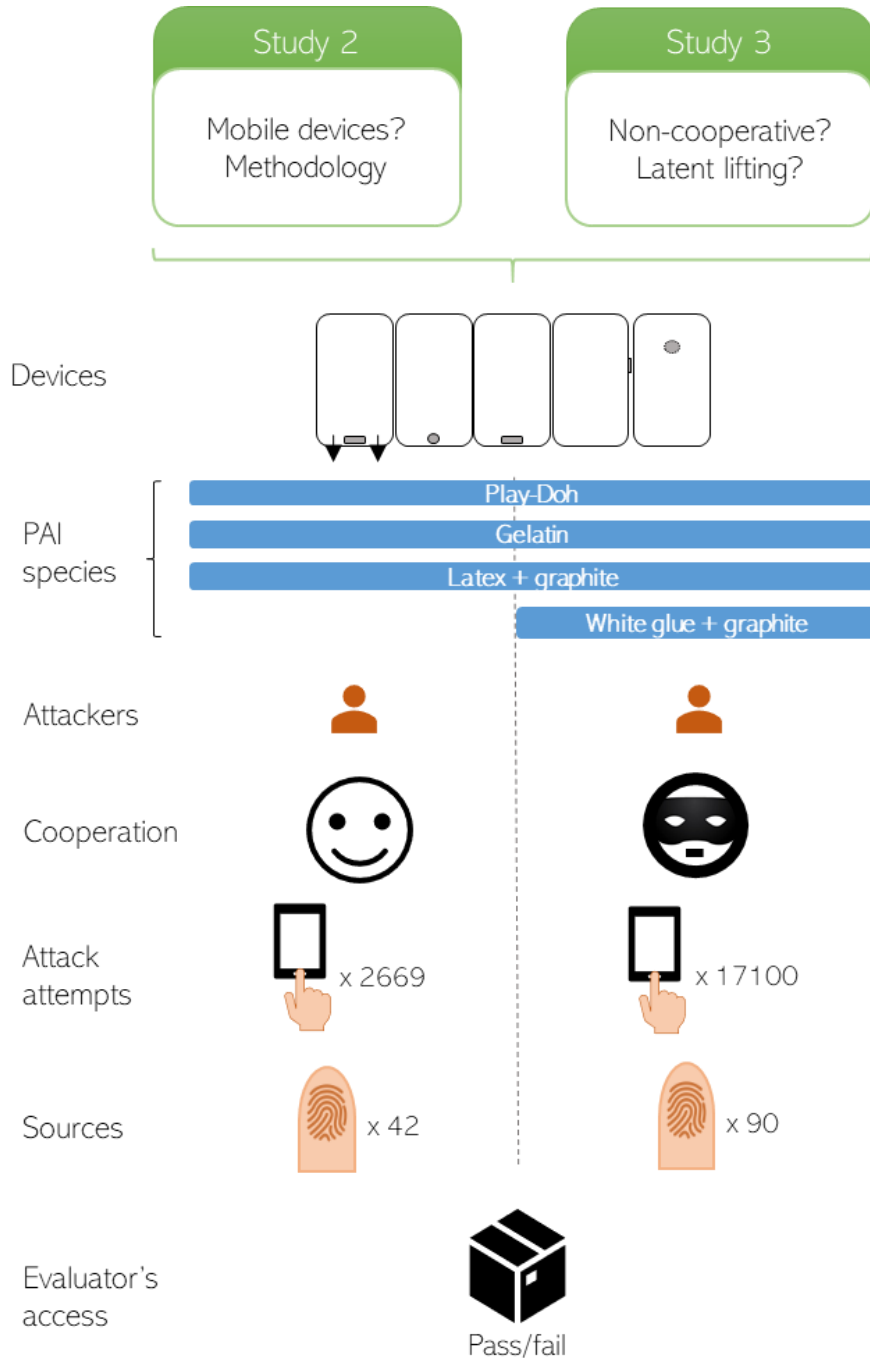
ON THE PREVIOUS chapter, experiments were performed to attack desktop fingerprint sensors. Thus, it was decided to start a series of experiments on smartphones with an embedded fingerprint reader, as it was a very unexplored area in the literature and they are widely used in society (Figure 21). For that end, 5 smartphones were put to the test by using fake fingers built with different materials in a cooperative and non-cooperative way. In both cases, a single expert performed the experiments (a different person for studies 2 and 3).



**Figure 21. Reasoning for evaluations on mobile devices performed by single expert attackers.**

The goal of study 2 was to perform and report a PAD evaluation with cooperative attacks on mobile devices, which had not been done, at least publicly. The same

experiment was performed again on study 3, but with non-cooperative attacks (Figure 22). Moreover, a novel technique to steal a latent fingerprint from a phone screen was found, which is the simplest to date, and thus, probably, the most threatening.



**Figure 22. Overview of evaluations on mobile devices performed by expert attackers. The symbol legend can be found on the List of Symbols.**

## 6.1 Planning

Both PAD evaluations on mobile devices were performed on 5 smartphones with different embedded fingerprint readers. Their main characteristics (sensor type, shape and location) can be seen on Table 30, as it was shown on Section 4.1.1. As it was mentioned in the methodology, the steps needed for the planning are identification of all possible threats and their corresponding attacks.

**Table 30. Identification of all possible threats and attacks: description of TOE.**

Sensor details					
	Mobile device (MD)	Sensor type	Sensor shape	Sensor location	Sensor technology
	MD1	Swipe	Rectangular	Front	Capacitive
	MD2	Touch	Circular	Front	Capacitive
	MD3	Touch	Rectangular	Front	Capacitive
	MD4	Touch	Rectangular	Side	Capacitive
MD5	Touch	Circular	Back	Capacitive	
Evaluator's access	Black box (pass/fail result) Full system				

**Table 31. Identification of all possible threats and attacks: description of target application.**

<b>Applications</b>	Unlock user’s smartphone. Access apps, e.g. bank accounts, password managers, personal pictures, etc.	
<b>Consequences of successful attack</b>	<ul style="list-style-type: none"> <li>• Unauthorized person unlocking another person’s smartphone.</li> <li>• No oversight while being used.</li> </ul>	
<b>Implemented functions</b>	<b>Enrollment:</b>	
	<ul style="list-style-type: none"> <li>• Real fingers</li> <li>• Different enrollment policies:</li> </ul>	
	<b>Mobile device</b>	<b>Attempt policy for enrollment</b>
	MD1	Around 10 attempts needed (can be extended 10 more times if wanted). Asks the user to move finger to get different samples and <b>checks it</b> .
	MD2	Around 15 attempts needed (10 for center part of the finger and 5 for corners). Asks the user to move finger to get different samples and <b>checks it</b> .
	MD3	Around 20 attempts needed. Asks the user to move finger to get different samples and <b>checks it</b> .
	MD4	Around 20 attempts needed. Asks the user to move finger to get different samples and <b>checks it</b> .
	MD5	Around 6 attempts needed. It just asks the user to move the finger to get different samples but <b>does not check it</b> .
	<b>Verification:</b>	
	<ul style="list-style-type: none"> <li>• Artefact attempts to be verified as the real finger that has been previously enrolled</li> <li>• Different verification policies:</li> </ul>	
	<b>Mobile device</b>	<b>Allowed failed attempts</b>
MD1	5	Waits for 30 seconds, can do attack again
MD2	3	Asks for PIN (blocked sensor needs PIN to unlock)
MD3	5	Waits for 30 seconds, can do attack again
MD4	5	Waits for 30 seconds, can do attack again
MD5	5	Waits for 30 seconds, can do attack again

As it can be seen, devices MD1, MD3, MD4 and MD5 accept an unlimited number of attempts to attack them, as when 5 attempts have failed, they just wait for 30 seconds and the attacker can try again, with no more restrictions (as far as the author’s knowledge). MD2 asks for a PIN after 3 attempts.

Also, for all cases, if the phone is turned off and the attacker wants to turn it on and access its data, he or she will need additional information apart from the bona-fide user’s fingerprint, like a PIN or a password. So, if the phone is found turned off or without power and the attacker does not know the user’s additional information, he or she will not be able to gain access.

The procedure for creating cooperative molds and artefacts has been widely reported on the literature [7], [10], [13], [45], so only a brief summary will be given here. It is the same procedure used for cooperative attacks on desktop readers from Section 5.1.2.

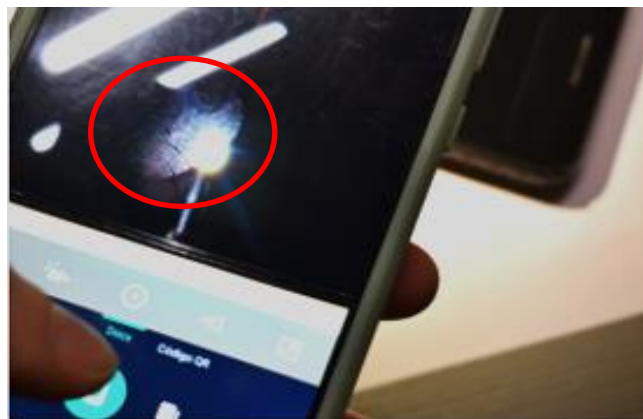


For cooperative attacks, the same process that was followed for the previous experiments is used for creating fake fingers. For non-cooperative attacks, a novel approach was found for this work. When people use their phones, they constantly leave fingerprints on the touch screen by the sheer interaction with it. Hence, it is possible for an attacker to steal these fingerprints if the genuine user's phone gets stolen. The technique used for acquiring these fingerprints is detailed as follows:

1. A latent fingerprint is left by the bonafide user on the smartphone screen. This is done in a manner that resembles a normal usage: the user taps briefly his or her finger on the surface, leaving a trace (Figure 23). Then, a freely available scanner app is used to take a picture with flash of the latent fingerprint (Figure 24). As it can be seen, the latent fingerprint is already very clear.

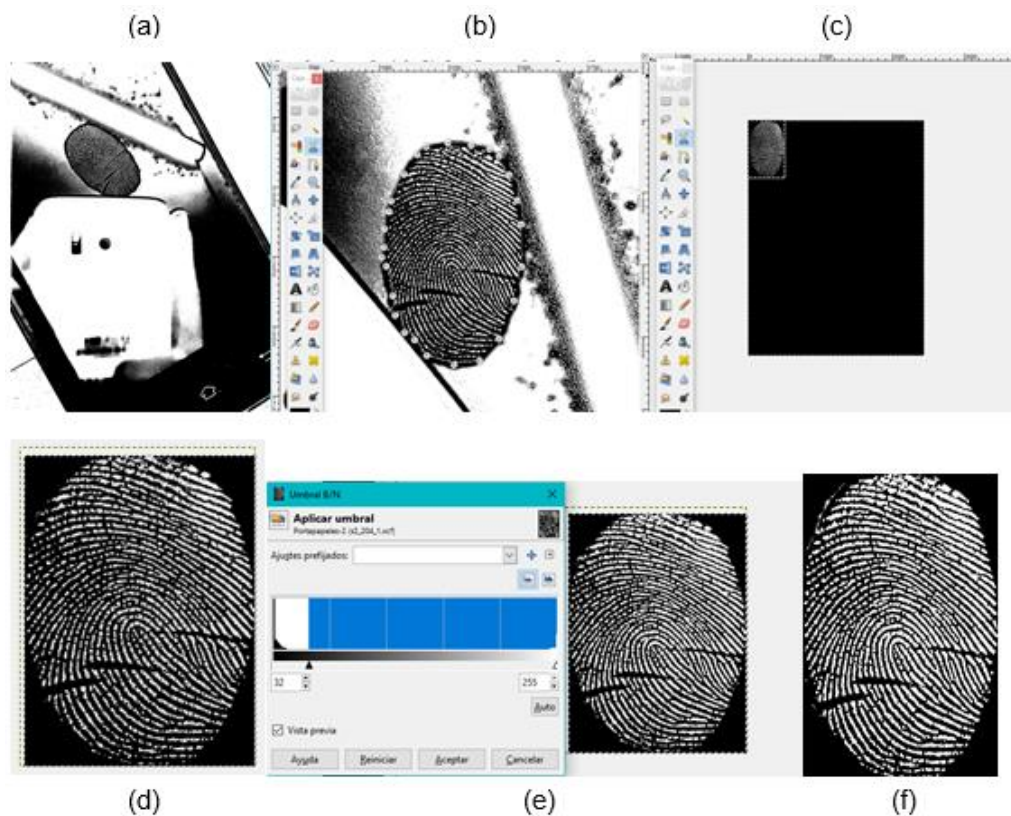


**Figure 23. Latent fingerprints left on the surface by tapping the genuine user's finger.**



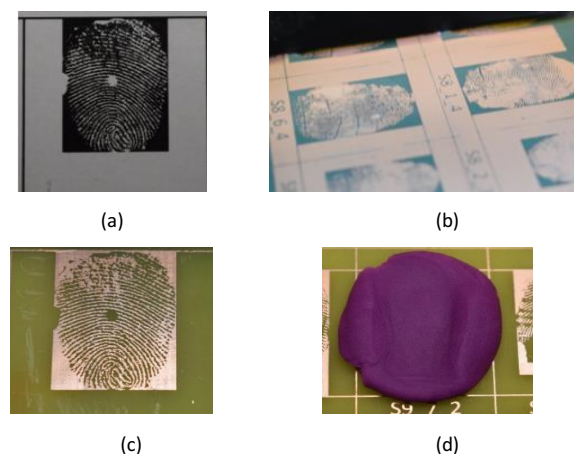
**Figure 24. Picture with flash being taken with the attacker's camera.**

2. For removing the background and minor retouching, freely available image editing programs can be used (Figure 25).



**Figure 25.** (a) Picture taken with scanner app with flash, where fingerprint is already visible. (b) Fingerprint zoomed in. (c) Background erased with image editing program, result on (d). (e) Threshold adjustment and (f) final result.

3. The mold is created by usual PCB developing techniques [13], and the artefacts are generated by the same methods used in non-cooperative attacks of Chapter 5 (Figure 26).



**Figure 26.** (a) Fingerprint image printed on a transparent sheet (b) PCB board being developed (c) Result after etching PCB board mold (d) Play-Doh artefact on the PCB mold.

A mobile app was made for iOS and Android (Figure 27). For acquiring the data, the visit screen is filled in by the evaluator (genuine user’s ID, attacker’s ID, device,

finger ID, type of attack and PAI species) and the app logs whether the attack succeeded or not. The enrollment was performed using the phone’s native settings procedure.

The screenshot shows a mobile application interface for logging PAD evaluation. It features several input fields and radio buttons:
 

- Bona-fide ID:** A text input field.
- Attacker ID:** A text input field.
- Gender:** Radio buttons for 'M' and 'F'.
- Device:** A text input field containing a blacked-out redaction.
- Finger:** A row of buttons labeled '1', '2', '3', '6', '7', and '8'.
- Type of attack:** Radio buttons for 'Coop' and 'Non-coop'.
- Artefact species:** Radio buttons for 'PLA', 'GEL', and 'LTX', followed by an 'Other' label and a text input field.
- START CAPTURE:** A prominent blue button at the bottom of the form.

**Figure 27. Smartphone app (Android and iOS) for logging the PAD evaluation. A pass/fail result is logged for each attempt.**

### 6.1.1 Analysis of attack potential

As it was explained on Section 4.1.2, the attack potential is a measure of the effort to be expended in attacking a TOE with a PAI, expressed in terms of an attacker’s expertise, resources and motivation, which can be divided into more specific parameters. In this way, TOEs are given a rating to assess their resistance to specific attacks, and it can be decided whether to add a PAD mechanism if these attacks are easy and probable. As explained previously, every threat has a corresponding attack. The particular case for this study can be seen on Table 32.

**Table 32. Planning: Analysis of attack potential by searching threats and their corresponding attacks (all studies on mobile devices).**

<b>Possible threats</b>	<ul style="list-style-type: none"> <li>• Only presentation attack: using an artefact generated from a user’s real finger on the sensor.</li> <li>• Intended operation of the system: unlock a smartphone, and thus accessing private data.</li> </ul>
<b>Possible attacks</b>	<ul style="list-style-type: none"> <li>• Corresponding attack: presentation attack.</li> <li>• Biometric characteristic can be obtained with or without cooperation from the capture subject. In this case, attacks were <b>cooperative</b>.</li> <li>• Level of expertise of the evaluator: proficient, although the materials needed for the evaluation can be found at any supermarket.</li> </ul>

### 6.1.1.1 Attack Potential calculation

Following the methodology already detailed on Section 4.1.2, the attack potential must be calculated to determine whether the TOE is resistant to attacks assuming a specific attack potential of an attacker. The calculation by score assignment for both studies can be seen on Table 33 and Table 34, respectively.

**Table 33. Attack Potential calculation for cooperative attacks on smartphone fingerprint sensors.**

COOPERATIVE ATTACKS					
	Preparation phase	PAI construction + exercising phase	Attack execution phase	Total factor rating	Score
Elapsed time	<1 day (capture subject is cooperative)	<1 day or <1 week (different material difficulty)	Few seconds (perform attack)	<1 week or <2 weeks	1.5
Expertise	Layman (information on effective materials widely available on internet)	Layman (easy to create)	Layman (not much expertise needed)	Layman	0
Knowledge of TOE	Public (well known on the internet that it works)	Public (manuals can be found on the internet)	Public (no knowledge needed)	Public	0
Window of opportunity	Unnecessary (no access to TOE needed)	Easy (access to TOE for practicing)	Easy (no oversight)	Easy	1
Equipment	Standard (materials easy to obtain at supermarkets or online)	Standard (but it is necessary to buy the TOE, which can be expensive)	Standard (no equipment needed)	Standard	2
<b>Overall attack rating</b>	<b>4.5 (Basic)</b>				
<b>Attack resistance</b>	<b>Minimum</b>				

**Table 34. Attack Potential calculation for non-cooperative attacks on smartphone fingerprint sensors.**

NON-COOPERATIVE ATTACKS					
	Preparation phase	PAI construction + exercising phase	Attack execution phase	Total factor rating	Score
Elapsed time	<1 week (capture subject is non-cooperative)	1 week (creating PAIs)	Few seconds (perform attack)	<2 weeks	2
Expertise	Layman (information on effective materials widely available on internet)	Proficient (process needs many steps)	Layman (not much expertise needed)	Proficient	3
Knowledge of TOE	Public (well known on the internet that it works)	Public (manuals can be found on the internet)	Public (no knowledge needed)	Public	0
Window of opportunity	Unnecessary (no access to TOE needed)	Easy (access to TOE for practicing)	Easy (no oversight)	Easy	1
Equipment	Standard (materials easy to obtain at supermarkets or online)	Standard (but it is necessary to buy the TOE, which can be expensive)	Standard (no equipment needed)	Standard	2
<b>Overall attack rating</b>	<b>8 (Basic)</b>				
<b>Attack resistance</b>	<b>Minimum</b>				

The overall attack rating is 4.5 (Basic) for the cooperative attacks and 8 (Basic) for the non-cooperative. Thus, the attacks would have to be considered in penetration testing for all evaluations assuming Minimum attack potentials (or higher). If penetration tests show that the attack is successful, the TOE would fail to resist against that attack potential.

### 6.1.2 Specification of penetration test

Once the TOE has been analyzed and described, the penetration test can be planned. The specifics for all studies on mobile devices can be seen on Table 35. The expert that performed the attacks is a different person for Studies 2 and 3.

**Table 35. Penetration test characteristics for the study on smartphone sensors performed by expert attackers.**

	<b>Cooperative (study 2)</b>	<b>Non-cooperative (study 3)</b>
<b>Capture subjects</b>	7	15
<b>Sources per capture subject (fingers)</b>	6 (index, middle and thumb from both hands)	
<b>Total sources (fingers)</b>	42	90
<b>Attempts per finger</b>	10	
<b>Total attempts</b>	2,669	17,100
<b>Sessions</b>	1 for bona fide 1 for attacks	
<b>Cooperation</b>	Cooperative	Non-cooperative
<b>PAI species</b>	3 (Play-Doh, gelatin, latex with graphite)	4 (Play-Doh, gelatin, latex with graphite, white glue with graphite)
<b>Molds</b>	Silicone	
<b>Evaluator's access</b>	Black box (pass/fail result)	
<b>Evaluator number and expertise</b>	1 expert	1 expert

## 6.2 Execution

As it was explained on Section 4.2, the execution can be done once the penetration test has been specified. It comprises three phases: detection, capture and processing.

### 6.2.1.1 Detection

Before the actual execution, the different PAI species were put to the test. If the sensor could detect the fingerprint, then it could be selected for the evaluation.

### 6.2.1.2 Capture

As checking the quality is not always possible for the evaluator, some artefacts with different qualities (examined by the evaluator) can be used to check which ones are obtained successfully by the reader and continue with that technique. Thus, the APCER metric given in the case of desktop sensors cannot be obtained here. In the case of mobile devices, some of them give a slight feedback on quality by telling the user that e.g. the finger is too wet. If an attacker is using a gelatin artefact and the smartphone prompts "finger too wet", the attacker will create another artefact with less proportion of water and try again.

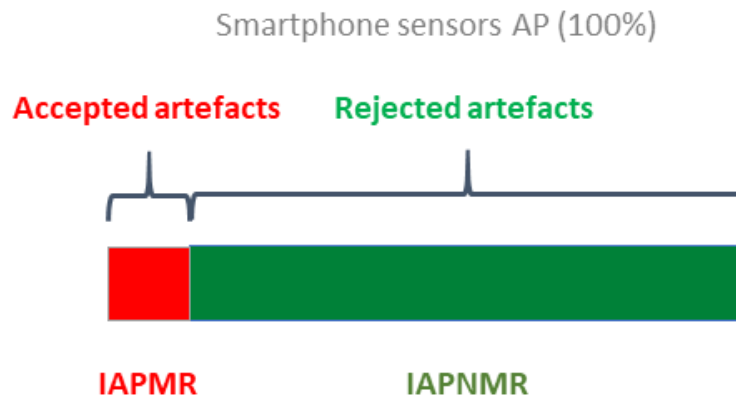
Lastly, it must be noted that each mobile device will have different algorithms, sensor technologies and quality and decision thresholds.

### 6.2.1.3 Processing

In the case of smartphones, being full systems with no access to intermediate data, no quality or similarity scores can be obtained, only pass/fail results. Thus, the data used for the posterior analysis was based solely on this.

## 6.3 Results

After the penetration test is executed, the results from the 4 evaluations can be obtained and analyzed. As it was explained on Section 4.3, the metrics to be used to report a full system (Figure 28) are IAPMR (Impostor Attack Presentation Match Rate) and its complementary, IAPNMR (Impostor Attack Presentation Non-Match Rate). These metrics apply to all evaluations on mobile devices.



**Figure 28. IAPMR and IAPNMR metrics, according to ISO/IEC 30107-3.**

As having successful PAIs is an undesirable outcome, the number of successful attacks will be represented in red, while unsuccessful attacks will be shown in green in all graphs.

### 6.3.1 Penetration test results

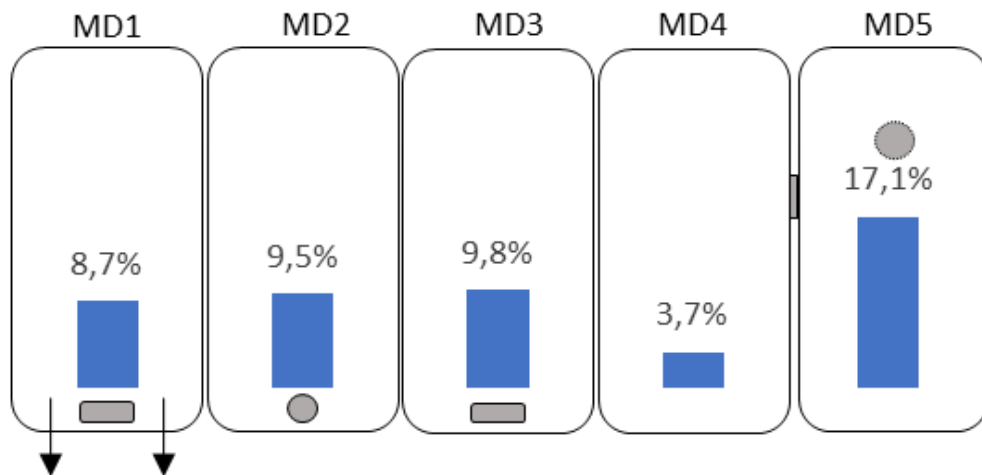
As it is important to obtain all the different nuances of the gathered results, several cases are analyzed for the penetration test:

- Results per device
- Results per device, per study
- Results per device, per PAI species

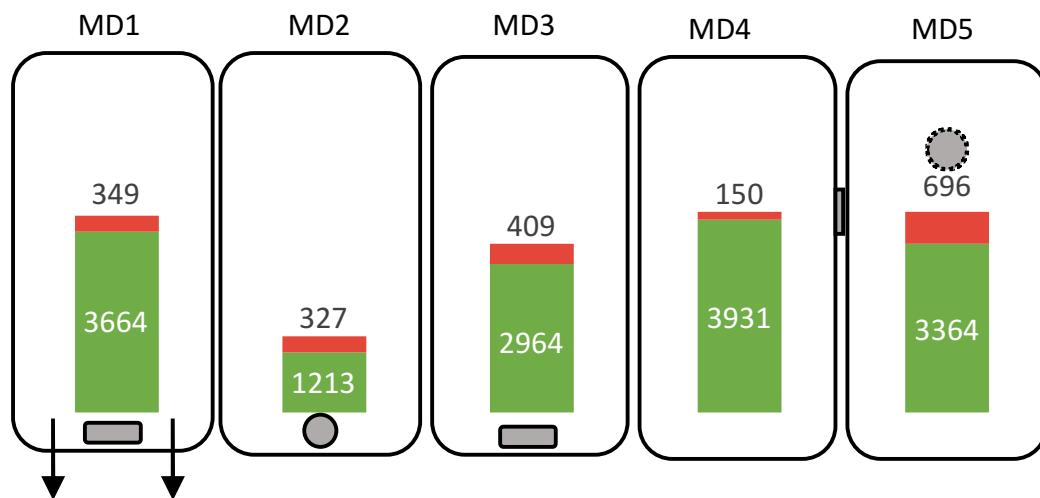
For every case, two separate graphs will be shown: IAPMR graph and fail/pass graph. IAPMR shows the proportion of successful attacks, but it is also important to discern how many attacks were performed in each case, as some experiments have far more attempts than others.

### 6.3.1.1 Results per device

This subsection gathers the overall presentation attack results for all mobile devices tested, both studies and all PAI species. For clarification purposes, these results will be shown inside the corresponding mobile device. The IAPMR for each device is represented on Figure 29 and the number of successful and unsuccessful attacks on Figure 30.



**Figure 29. IAPMR per device, studies 2 and 3 together.**



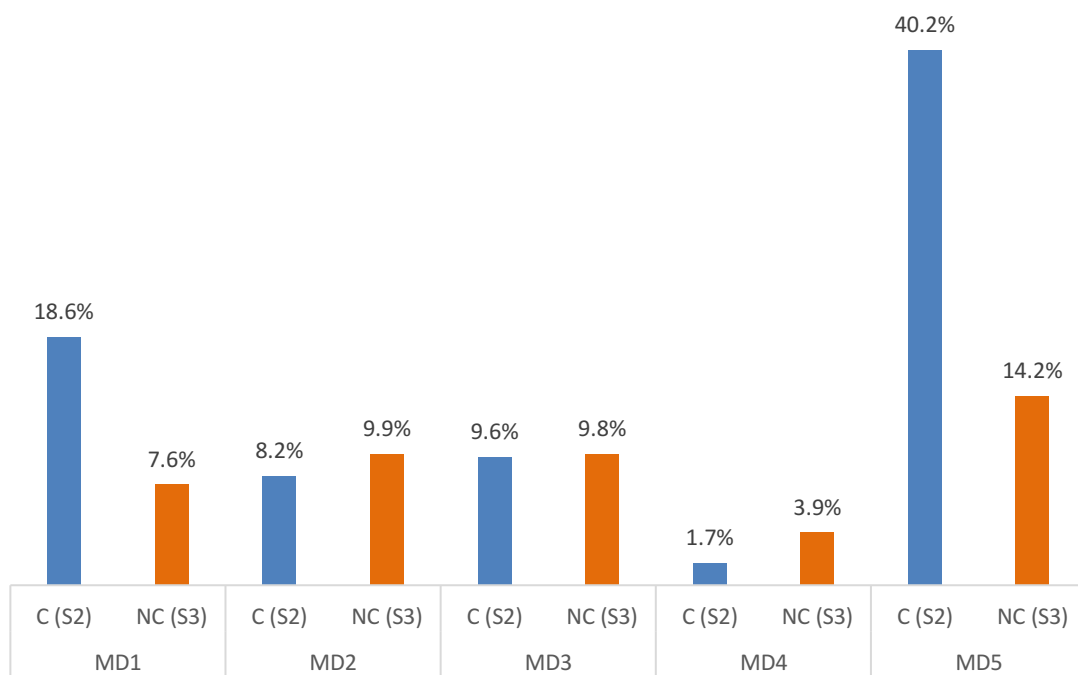
**Figure 30. Number of successful (in red) and failed (in green) attacks for each mobile device. Studies 2 and 3 together.**

As it can be observed, the most vulnerable mobile device overall is MD5 with a 17.1% of successful presentation attacks and the least vulnerable is MD4 with 3.7%. The rest of the mobile devices had an IAPMR of 8.7-9.8%. The smartphone with the least amount of attacks is MD2. This is because most attack attempts resulted in feedback from the system (“finger too wet”, etc.). This could be considered a quality feedback

which influences the final results, because the attacker can improve his or her technique based on these messages.

### 6.3.1.2 Results per device, per study

This subsection analyzes the difference between both studies. As it was explained previously, both studies are performed by an expert (a different one for each case), but study 2 covers cooperative attacks and study 3 non-cooperative. Thus, the results of each study are separated in Figure 31 and Figure 32.



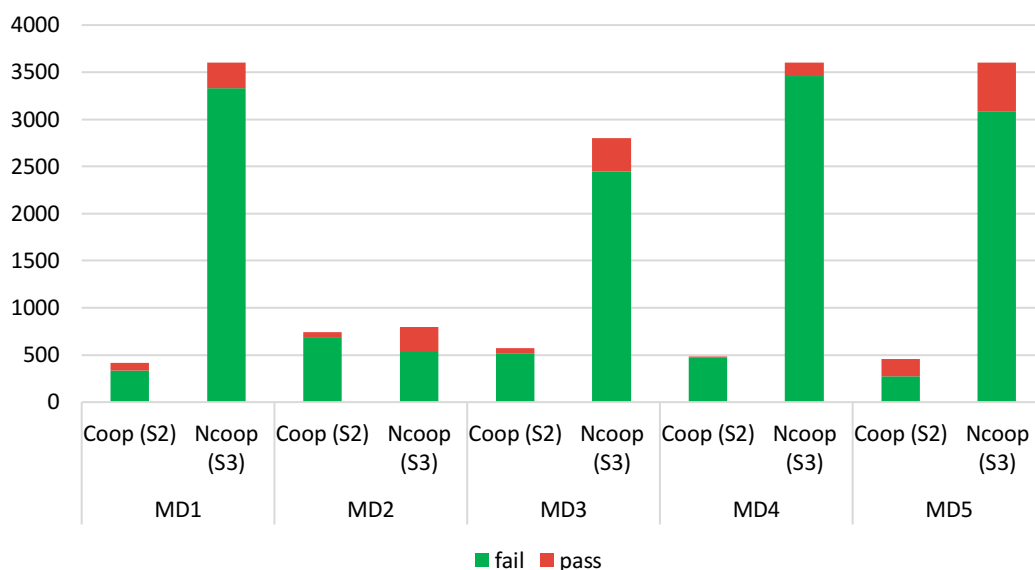
**Figure 31. IAPMR per device (MD1-MD5) and per study (2-3). C = cooperative attacks (study 2) and NC = non-cooperative attacks (study 3).**

Initially, non-cooperative attacks should be less successful than cooperative ones, as the techniques used to obtain the fingerprint are less accurate for the former case (lifting a latent fingerprint versus the capture subject willingly laying the finger on a special mold material). Nevertheless, this difference is not clear in these studies: for MD1 and MD5, the cooperative attacks are clearly more successful; for MD2 and MD3, the success rate is very similar; for MD4, the non-cooperative attacks worked more times than the cooperative ones. This last outcome is due to the PAI species used: white glue with graphite was not used for the cooperative attacks, and it was very successful in attacking MD4. White glue with graphite was not good at performing attacks on study 1 (experiment performed on desktop sensors on Section 5.1.2), so it was not considered for study 2 (cooperative attacks on mobile devices). When a second expert laid out the penetration test for study 3 (non-cooperative attacks on mobile devices), it was decided to also try this material because it had been reported to work on [16].

It must also be noted that a significantly higher number of attacks were carried out on study 3, with 17,100 attacks versus the 2,669 for study 2. The number of total failed



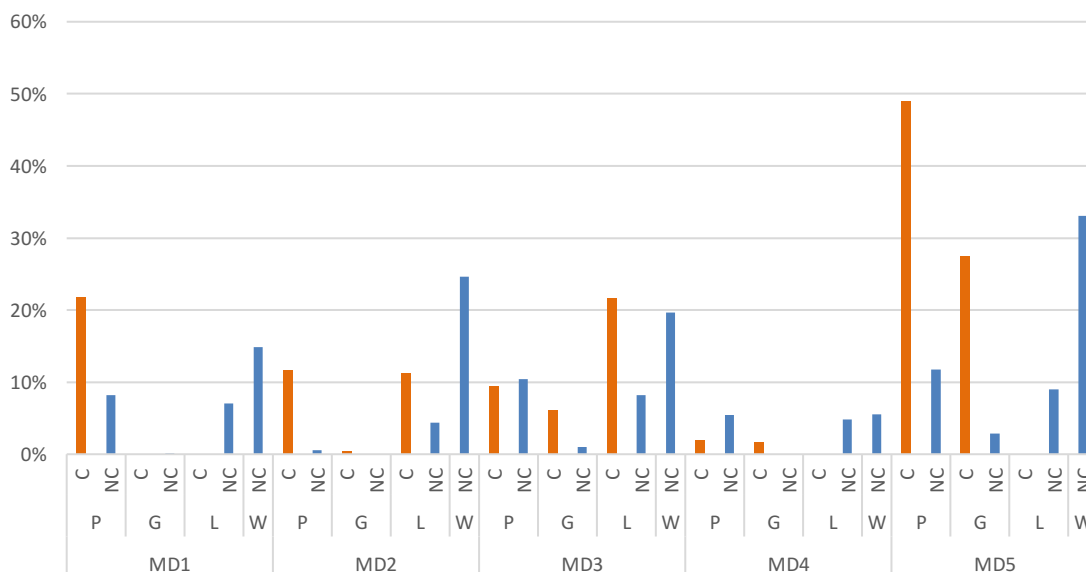
and successful attacks can be seen on Figure 32. This means that the evaluator could have obtained an increasing expertise along the experiment.



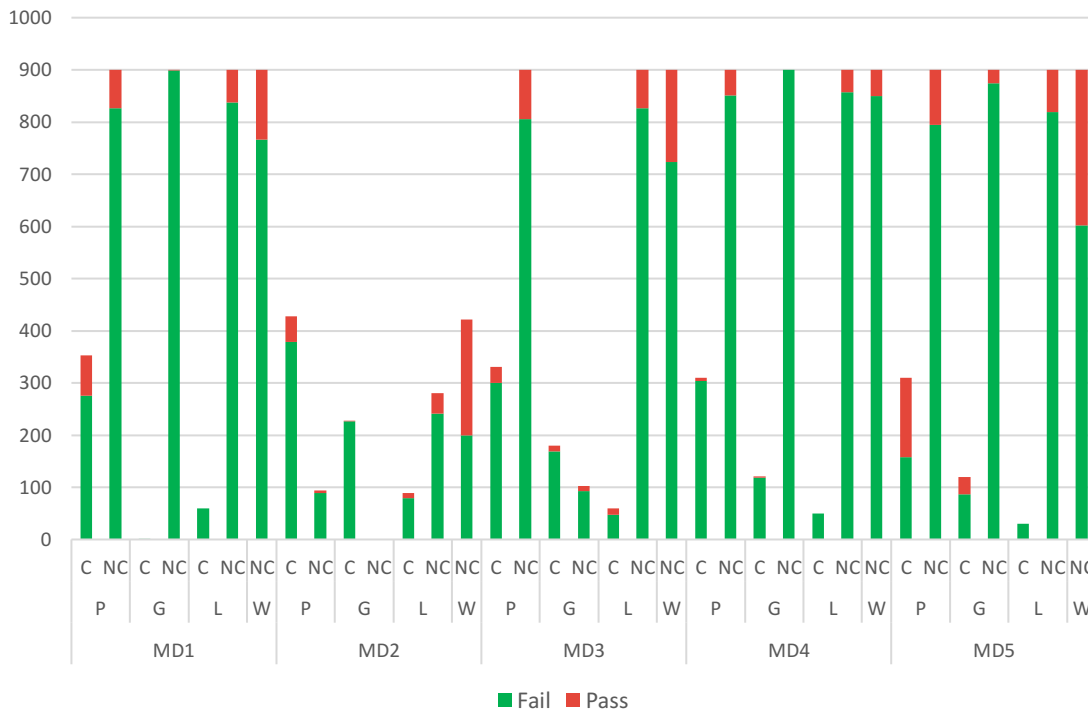
**Figure 32.** Number of successful (in red) and failed (in green) attacks for each mobile device, divided by study and cooperation type.

### 6.3.1.3 Results per device, per PAI species

As it was stated previously, the common PAI species for both studies are Play-Doh, gelatin and latex with graphite. In addition, for study 3, white glue with graphite was used. The results by study and by PAI species can be observed on Figure 33 and Figure 34.



**Figure 33.** IAPMR per device, per study and per PAI species. C = cooperative attacks (study 2) and NC = non-cooperative attacks (study 3). P = Play-Doh, G = gelatin, L = latex with graphite and W = white glue with graphite.



**Figure 34. Number of successful (red) and failed (green) attacks by study, device and PAI species. C = cooperative attacks (study 2) and NC = non-cooperative attacks (study 3). P = Play-Doh, G = gelatin, L = latex with graphite and W = white glue with graphite.**

Play-Doh was successful at least once on both studies, all devices. Gelatin was less consistently successful: it did not achieve any successful attack on MD1 (study 2) and MD2 (study 3). Latex with graphite was successful in attacking MD2 and MD3 in both studies, and could not attack MD1, MD4 and MD5 for study 2. White glue with graphite could also hack all mobile devices, although it was only used non-cooperatively. Overall, it can be clearly seen that Play-Doh was very successful on MD5, obtaining an IAPMR of 49%.

### 6.3.2 Vulnerability test results

As it was explained on Section 4.3.1, once all the data has been analyzed after the penetration test, the evaluator shall report which PAI species were successful in attacking each system to report their found vulnerabilities to presentation attacks. The result for these experiments is shown on Table 36.

**Table 36. List of vulnerabilities of smartphones. Not all PAI species were tried on every phone and that different numbers of attempts were performed on each experiment.**

PAI species	MD1	MD2	MD3	MD4	MD5
Play-Doh	x	x	x	x	x
Gelatin	x	x	x	x	x
Latex + graphite	x	x	x	x	x
White glue + graphite	x	x	x	x	x

As it can be seen, all mobile devices were successfully attacked at least once with all PAI species. The consequences that may derive from these vulnerabilities are that an attacker could unlock the phone and have access to all the apps that do not require additional security, which are most of them at the time this document was written.

## 6.4 Conclusions

In this chapter, 2 evaluations were performed on smartphones that have an embedded fingerprint sensor. Each study had different questions in mind. First, with the knowledge gathered from the evaluation of Chapter 5 with desktop readers, a PAD evaluation was performed on 5 smartphones with an embedded fingerprint sensor. This decision was taken because no previous public evaluations had been performed on mobile devices, which are increasingly being used in our everyday lives. The first evaluation was done by one expert in a cooperative manner. Then, a different expert performed a very similar PAD evaluation, following the same methodology and on the same mobile devices, but in a non-cooperative way. Moreover, a novel technique was used to steal fingerprints from capture subjects, simpler than any other reported on the literature. Throughout the process, some lessons were learnt:

- Some devices give slight feedback of the quality (“finger too wet”, etc.). This can help an attacker when creating PAIs. For instance, if a gelatin artefact is used on a capture device and the phone shows a feedback message that says, “finger too wet”, the attacker will rebuild the gelatin fingers using a smaller proportion of water.
- Some devices allow an unlimited number of attempts to present a sample, giving the attacker unlimited chances. This can be fixed by asking for additional information (PIN, password, another biometric modality).
- IAPMR (Impostor Attack Presentation Match Rate) is dependent on the evaluator’s ability to create artefacts and on the capture subject. Thus, it is important to use as many attackers and capture subjects as possible when evaluating PAD in mobile devices.
- MD5 uses only 6 captures for enrollment (while other devices use more than 15), and this could be a reason why it is more vulnerable to attacks than the others.
- On study 3, it was found that stealing someone’s fingerprint is simpler than it was thought, as all 5 smartphones were successfully attacked with a non-cooperative approach, using the most common materials from the literature. For all mobile devices, 3 out of 4 materials used successfully attacked the sensors.

Nevertheless, it must be noted that even if an attacker can gain access to the smartphone, he or she will not be able to change passwords or add his or her own fingerprint to the system, as a PIN or password is needed for those actions. Moreover, if the attacker finds the smartphone when it’s shut down, he or she will also need a PIN or password to unlock it the first time. As a general consideration, it must be noted that including a fingerprint reader in smartphones greatly increased the security of mobile devices. The reason is that people that had never set up a PIN or password on their phones (due to being uncomfortable or a nuisance) started using the fingerprint sensor easily, adding an important layer of protection to their personal phones.

## 6.5 Contributions and dissemination

Both studies on PAD assessment of mobile devices were published in journal and conference papers. Moreover, several contributions were accepted in the pertinent international standard ISO/IEC 30107-4 Biometric Presentation Attack Detection – Part 4: *Profile for evaluation of mobile devices*.

### 6.5.1 Journal papers

[95] I. Goicoechea-Telleria, R. Sanchez-Reillo, J. Liu-Jimenez, and R. Blanco-Gonzalo, “Attack Potential Evaluation in Desktop and Smartphone Fingerprint Sensors: Can They Be Attacked by Anyone?,” *Hindawi*, vol. 2018, pp. 1–13, 2018.

- Along with study 1 of Chapter 5, an attack potential analysis was carried out for PAD evaluations.

### 6.5.2 Conference papers

[22] I. Goicoechea-Telleria, J. Liu-Jimenez, R. Sanchez-Reillo, and W. Ponce-Hernandez, “Vulnerabilities of Biometric Systems integrated in Mobile Devices : an evaluation,” *IEEE Int. Carnahan Conf. Secur. Technol.*, 2016.

- Contribution of developing a methodology for PAD evaluation on mobile devices and then performing an evaluation following it.

[97] I. Goicoechea-Telleria, A. Garcia-peral, A. Husseis, and R. Sanchez-reillo, “Presentation Attack Detection Evaluation on Mobile Devices : Simplest Approach for Capturing and Lifting a Latent Fingerprint,” in *International Carnahan Conference on Security Technology (ICCST)*, 2018.

- Contribution of performing a PAD evaluation on mobile devices using non-cooperative attacks and finding and using a novel approach to steal latent fingerprints from a capture subject.

### 6.5.3 Standardization

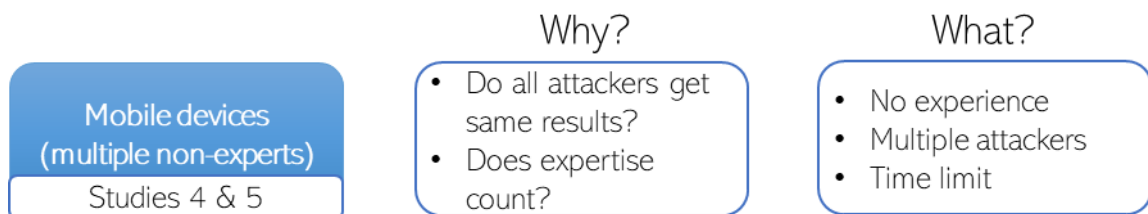
[2] SC 37, “ISO/IEC 2nd WD 30107-4 Biometric presentation attack detection - Part 4: Profile for evaluation of mobile devices,” 2018.

- Contributions on feedback, enrollment and verification policies and description requirements.

## Chapter 7. Presentation Attack Detection evaluation on mobile devices - multiple non-experts

---

THE PREVIOUS CHAPTER covered two PAD evaluations performed on mobile devices by two different experts. This gave rise to two questions: do all attackers get the same results when attacking a biometric system? Does expertise count? (Figure 35). With this in mind, it was decided to give the same smartphones to several different attackers with no previous knowledge on Biometrics and let them attempt to attack them. The goal was also to find additional materials that could be successful in fooling fingerprint sensors.



**Figure 35. Reasoning for evaluations on mobile devices performed by multiple non-expert attackers.**

For study 4, 36 attackers with no background in Biometrics were given one week to attack one smartphone's fingerprint reader (6 smartphones in total, same ones than in the second study). Each had to, at least, use 3 bona fide capture and use each material

at least 120 times on the smartphone sensor, making a total of 10,034 attempts. As more than one week would be needed to create non-cooperative fake fingers, the study was focused only on cooperative attacks.

For study 5, a similar task was given to an additional 10 non-experts in spoofing, but in a hackathon setting. This entails that the participants did not perform a thorough evaluation with a set protocol, but instead tried many different materials for artefacts. Thus, the goal of this study is to find out which material combinations were able to hack the device at least once, and to see if smartphones can be hacked by novel attackers in a short time. Working in groups of three or four, each team was given the task to experiment with the creation of a series of fake fingers in an attempt to unlock smartphones. They could ask for any material from the supermarket or Amazon to complete this task, so that the attack potential stays low. Before the hackathon, they had one week to research methods and materials. For development and testing, they had a 12-hour limit.

For both studies, the starting point for the participants was a video of an expert (the one from study 1) creating molds and artefacts, along with papers on the subject. An overview of both studies can be seen on Figure 36. Due to the nature of the hackathon (time limit), some evaluation protocol characteristics from study 5 are not available. Moreover, at the beginning of the hackathon (study 5), one of the smartphones broke and its evaluation could not be performed.

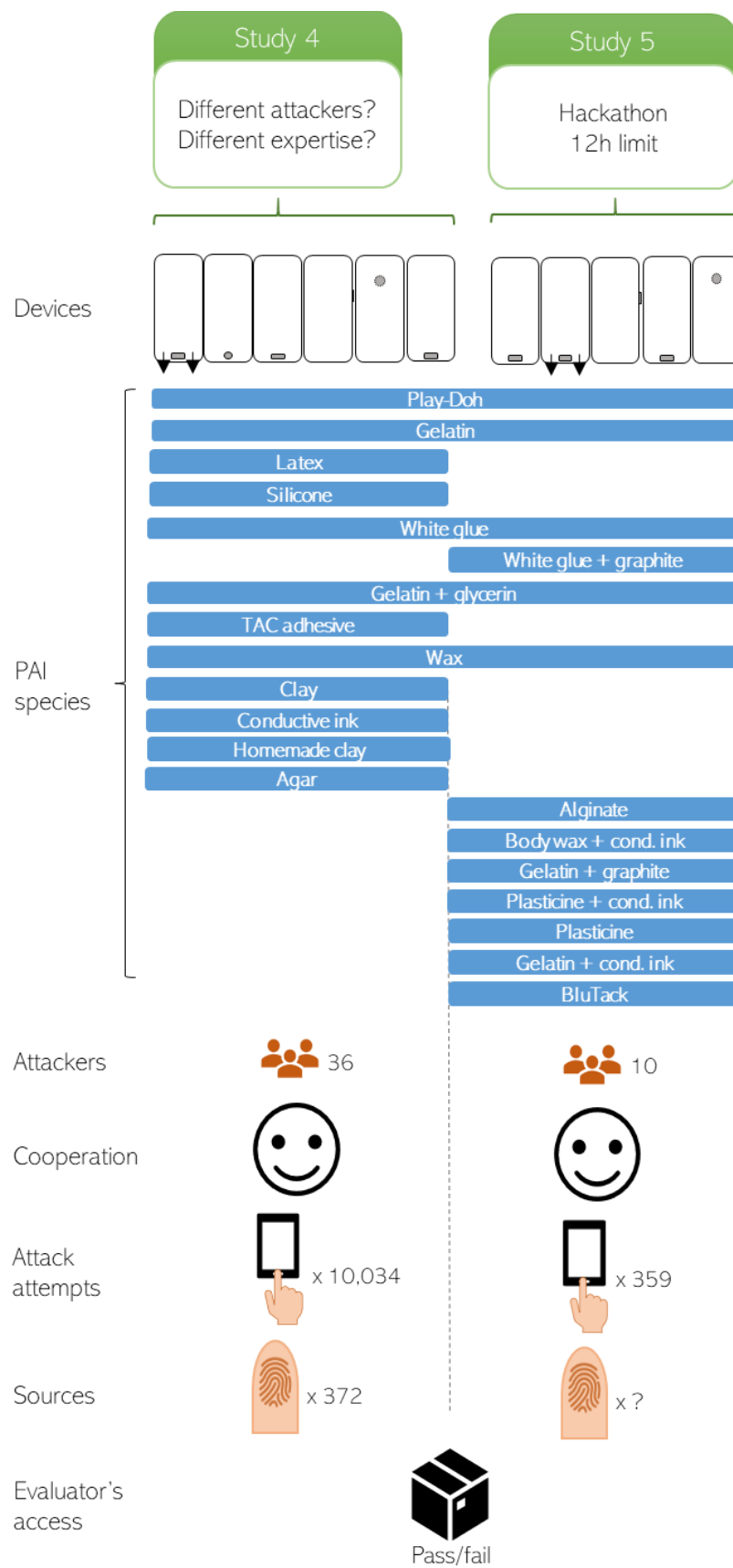


Figure 36. Overview of evaluations on mobile devices performed by multiple non-expert attackers.

## 7.1 Planning

For the case of the third study, we gathered 36 inexperienced attackers with no background in attacking biometric systems. We prepared a process or “recipe” they had to follow to create the artefacts and we gave it to them on writing and video. They had to create artefacts with Play-Doh and gelatin but could get extra points for using more PAI species. Again, there were 6 smartphones available for the evaluation and each simulated attacker was given one at random. Also, those who owned one of these cell phones could use them for the attack. Thus, some smartphones were used more than others. They had one week to perform at least 120 attack attempts per PAI species. To make sure that they were performing the evaluation correctly, attackers had to record themselves on video using the fake fingers on the sensors. Moreover, they had to take pictures of all molds and artefacts, and finally had to hand over a box with all of them. A similar experiment was performed for study 5 in the shape of a hackathon: participants had 1 week to research attack methods and 12 hours to perform the attacks, including PAI preparation.

PAD evaluations on mobile devices were performed on 6 smartphones with different embedded fingerprint readers. Their main characteristics (sensor type, shape and location) can be seen on Table 37. The description of the target application is detailed on Table 38.

**Table 37. Identification of all possible threats and attacks: description of TOE.**

<b>Sensor details</b>				
	<b>Mobile device (MD)</b>	<b>Sensor type</b>	<b>Sensor shape</b>	<b>Sensor location</b>
	MD1	Swipe	Rectangular	Front
	MD2	Touch	Circular	Front
	MD3	Touch	Rectangular	Front
	MD4	Touch	Rectangular	Side
	MD5	Touch	Circular	Back
MD6	Touch	Rectangular	Front	
<b>Evaluator’s access</b>	Black box (pass/fail result) Full system			



**Table 38. Identification of all possible threats and attacks: description of target application.**

<b>Applications</b>	Unlock user's smartphone. Access apps, e.g. bank accounts, password managers, personal pictures, etc.	
<b>Consequences of successful attack</b>	<ul style="list-style-type: none"> <li>• Unauthorized person unlocking another person's smartphone.</li> <li>• No oversight while being used.</li> </ul>	
<b>Implemented functions</b>	<b>Enrollment:</b>	
	<ul style="list-style-type: none"> <li>• Real fingers</li> <li>• Different enrollment policies:</li> </ul>	
	<b>Mobile device</b>	<b>Attempt policy for enrollment</b>
	MD1	Around 10 attempts needed (can be extended 10 more times if wanted). Asks the user to move finger to get different samples and <b>checks it</b> .
	MD2	Around 15 attempts needed (10 for center part of the finger and 5 for corners). Asks the user to move finger to get different samples and <b>checks it</b> .
	MD3	Around 20 attempts needed. Asks the user to move finger to get different samples and <b>checks it</b> .
	MD4	Around 20 attempts needed. Asks the user to move finger to get different samples and <b>checks it</b> .
	MD5	Around 6 attempts needed. It just asks the user to move the finger to get different samples but <b>does not check it</b> .
	<b>Verification:</b>	
	<ul style="list-style-type: none"> <li>• Artefact attempts to be verified as the real finger that has been previously enrolled</li> <li>• Different verification policies:</li> </ul>	
	<b>Mobile device</b>	<b>Allowed failed attempts</b>
MD1	5	Waits for 30 seconds, can do attack again
MD2	3	Asks for PIN (blocked sensor needs PIN to unlock)
MD3	5	Waits for 30 seconds, can do attack again
MD4	5	Waits for 30 seconds, can do attack again

For the evaluation, the same smartphone app is used to log the attempts carried out by the attackers. For more details, refer to Chapter 6. The procedure for creating cooperative molds and artefacts is the same procedure used for cooperative attacks on desktop readers from Section 5.1.2.

### 7.1.1 Analysis of attack potential

As it was explained on Section 4.1.2 *Analysis of Attack Potential*, the attack potential is a measure of the effort to be expended in attacking a TOE with a PAI, expressed in terms of an attacker's expertise, resources and motivation, which can be divided into more specific parameters. In this way, TOEs are given a rating to assess their resistance to specific attacks. As explained previously, every threat has a corresponding attack. The particular case for this study can be seen on Table 39.

**Table 39. Planning: Analysis of attack potential by searching threats and their corresponding attacks (all studies on mobile devices).**

<b>Possible threats</b>	<ul style="list-style-type: none"> <li>• Only presentation attack: using an artefact generated from a user’s real finger on the sensor.</li> <li>• Intended operation of the system: unlock a smartphone, and thus accessing private data.</li> </ul>
<b>Possible attacks</b>	<ul style="list-style-type: none"> <li>• Corresponding attack: presentation attack.</li> <li>• Biometric characteristic can be obtained with or without cooperation from the capture subject. In this case, attacks were <b>cooperative</b>.</li> <li>• Level of expertise of the evaluator: proficient, although the materials needed for the evaluation can be found at any supermarket.</li> </ul>

### 7.1.1.1 Attack Potential calculation

Following the methodology already detailed on Section 4.1.2, the attack potential must be calculated to determine whether the TOE is resistant to attacks assuming a specific attack potential of an attacker. The calculation by score assignment for both studies can be seen on Table 40. All materials result in the same attack potential score, as all of them take less than 1 week to build, even for inexperienced attackers.

**Table 40. Attack Potential calculation for cooperative attacks on smartphone fingerprint sensors.**

COOPERATIVE ATTACKS					
	Preparation phase	PAI construction + exercising phase	Attack execution phase	Total factor rating	Score
Elapsed time	<1 day (capture subject is cooperative)	<1 day or <1 week (different material difficulty)	Few seconds (perform attack)	<1 week or <2 weeks	1.5
Expertise	Layman (information on effective materials widely available on internet)	Layman (easy to create)	Layman (not much expertise needed)	Layman	0
Knowledge of TOE	Public (well known on the internet that it works)	Public (manuals can be found on the internet)	Public (no knowledge needed)	Public	0
Window of opportunity	Unnecessary (no access to TOE needed)	Easy (access to TOE for practicing)	Easy (no oversight)	Easy	1
Equipment	Standard (materials easy to obtain at supermarkets or online)	Standard (but it is necessary to buy the TOE, which can be expensive)	Standard (no equipment needed)	Standard	2
<b>Overall attack rating</b>	<b>4.5 (Basic)</b>				
<b>Attack resistance</b>	<b>Minimum</b>				

The overall attack rating is 4.5 (Basic) for the cooperative ones. Thus, the attacks would have to be considered in penetration testing for all evaluations assuming Minimum attack potentials (or higher). If penetration tests show that the attack is successful, the TOE would fail to resist against that attack potential.

### 7.1.2 Specification of penetration test

Once the TOE has been analyzed and described, the penetration test can be planned. The specifics for all studies on mobile devices can be seen on Table 41.

**Table 41. Penetration test characteristics for the study on smartphone sensors performed by multiple non-expert attackers.**

	<b>Study 4</b>	<b>Study 5 (hackathon)</b>
<b>Capture subjects</b>	115	? (no information from participants)
<b>Sources per capture subject (fingers)</b>	6 (index, middle and thumb from both hands)	
<b>Total sources (fingers)</b>	372	? (no information from participants)
<b>Attempts per finger</b>	10	? (no information from participants)
<b>Total attempts</b>	10,034	359
<b>Sessions</b>	1 for bona fide 1 for attacks	
<b>Cooperation</b>	Cooperative	
<b>PAI species</b>	12 (Play-Doh, gelatin, gelatin with glycerin, silicone, TAC adhesive, wax, clay, wood glue, conductive ink, latex, homemade clay, agar)	13 (Play-Doh, gelatin, white glue, white glue + graphite, gelatin + glyceryn, wax, alginate, body wax + conductive ink, gelatin + graphite, plasticine + conductive ink, plasticine, gelatin + conductive ink, BluTack)
<b>Molds</b>	Silicone	BluTack, wax, hot glue, plasticine, Play-Doh, silicone, stamp wax
<b>Evaluator's access</b>	Black box (pass/fail result)	
<b>Evaluator number and expertise</b>	36 non-experts	10 non-experts

#### 7.1.2.1.1 Execution

As it was explained on Section 4.2, the execution can be done once the penetration test has been specified. It comprises three phases: detection, capture and processing.

#### 7.1.2.2 Detection

Before the actual execution, the different PAI species were put to the test. If the sensor could detect the fingerprint, then it could be selected for the evaluation.

#### 7.1.2.3 Capture

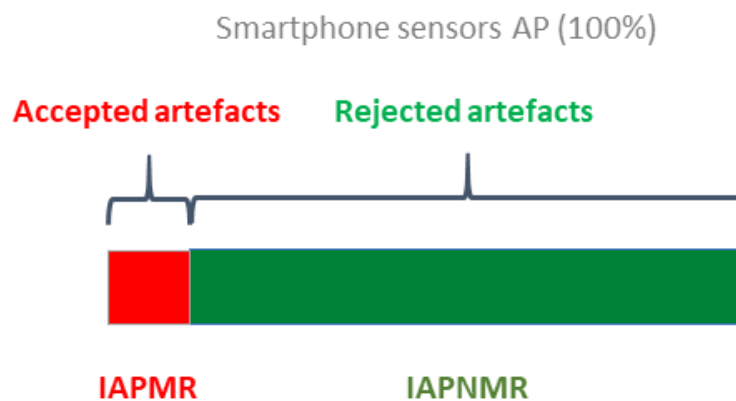
As it was mentioned on the previous chapter, checking the quality is not always possible for the evaluator. Also, each mobile device will have different algorithms, sensor technologies and quality and decision thresholds.

#### 7.1.2.4 Processing

In the case of smartphones, being full systems with no access to intermediate data, no quality or similarity scores can be obtained, only pass/fail results. Thus, the data used for the posterior analysis was based solely on this.

## 7.2 Results

After the penetration test is executed, the results from both experiments can be obtained and analyzed. As it was explained on Section 4.3, the metrics to be used to report a full system (Figure 37) are IAPMR (Impostor Attack Presentation Match Rate) and its complementary, IAPNMR (Impostor Attack Presentation Non-Match Rate). This applies to all full-system evaluations performed on smartphones.



**Figure 37. IAPMR and IAPNMR metrics, according to ISO/IEC 30107-3.**

As having successful PAIs is an undesirable outcome, the number of successful attacks will be represented in red, while unsuccessful attacks will be shown in green in all graphs.

### 7.2.1 Penetration test results

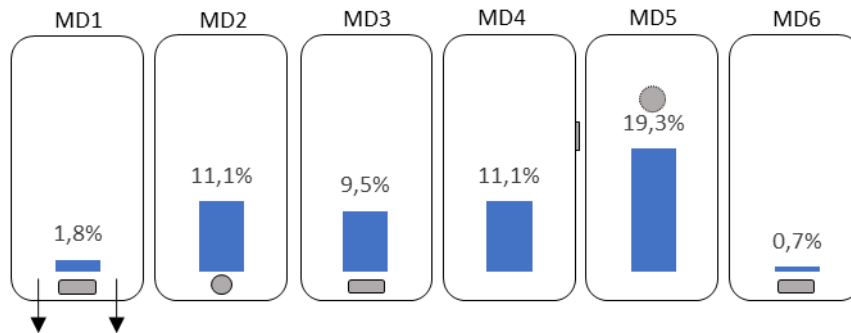
As it is important to obtain all the different nuances of the gathered results, several cases are analyzed for the penetration test:

- Results per device
- Results per device, per study
- Results per device, per attacker
- Results per device, per PAI species

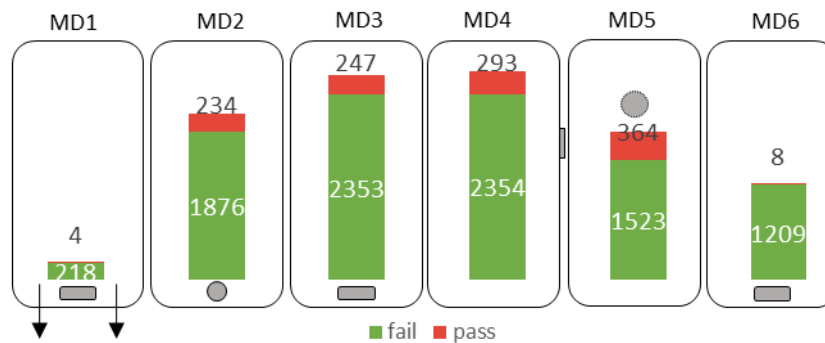
For every case, two separate graphs will be shown: IAPMR graph and fail/pass graph. IAPMR shows the proportion of successful attacks, but it is also important to discern how many attacks were performed in each case, as some experiments have far more attempts than others.

### 7.2.1.1 Results per device

This subsection gathers the overall presentation attack results for all mobile devices tested, both studies and all PAI species. For clarification purposes, these results will be shown inside the corresponding mobile device. The IAPMR for each device is represented on Figure 29 and the number of successful and unsuccessful attacks on Figure 30.



**Figure 38. IAPMR per device, both experiments together.**

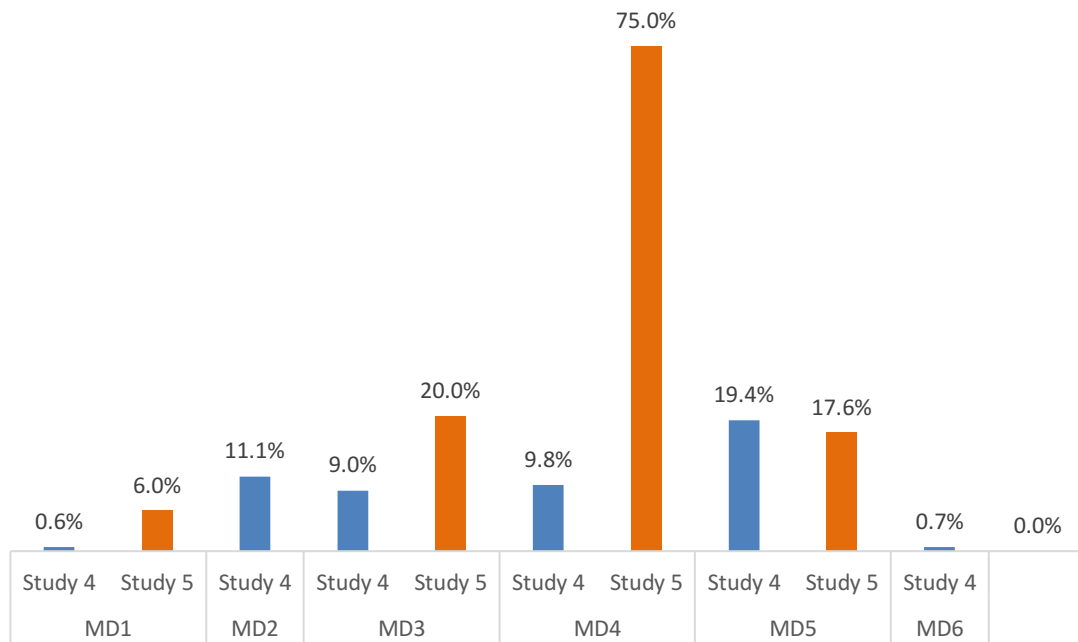


**Figure 39. Number of successful (in red) and failed (in green) attacks for each mobile device. Both experiments together.**

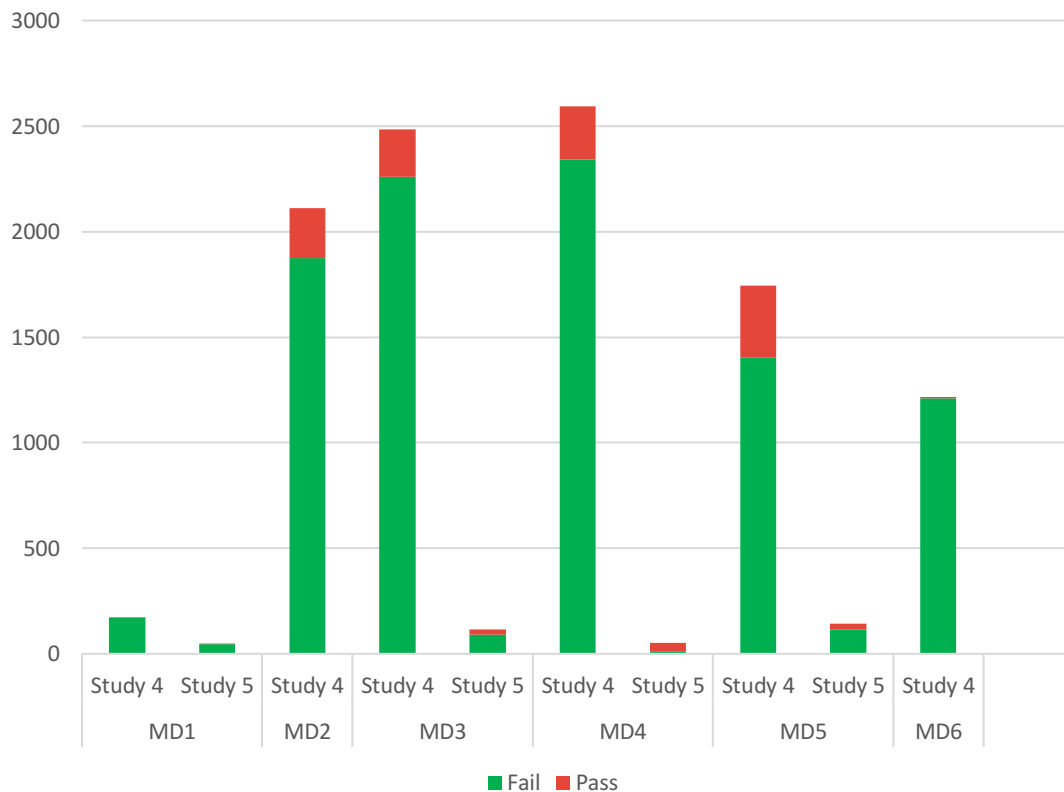
As it can be observed, the most vulnerable mobile device overall is MD5 with a 19.3% of successful presentation attacks and the least vulnerable is MD6 with 0.7%, followed closely by MD1 with 1.8%. MD4 was the device with the highest number of attack attempts: 293 successful and 2,354 unsuccessful. As it can be seen, there is a big difference in the number of attack attempts, as MD1 only had 222 total tries. This is because the attackers had a high difficulty placing the PAI on the sensor without breaking it (swipe sensor).

### 7.2.1.2 Results per device, per study

This subsection analyzes the difference between studies. Even though both experiments were performed by multiple non-experienced attackers, the goal of study 4 was to follow a set evaluation protocol and experiment for one week, while the goal of study 5 was to find PAI species that worked on the sensors within a 12-hour limit. Thus, the results of each study are separated in Figure 40 and Figure 41.



**Figure 40. IAPMR per device (MD1-MD6) and per study (4-5).**



**Figure 41. Number of successful (in red) and failed (in green) attacks for each mobile device, divided by study.**

Notably, the experiments performed on MD4 on study 5 are the most successful (75% IAPMR), in high contrast with the other test. Nevertheless, on the fail/pass

complementary graph (Figure 41), it can be seen that very few experiments were done on study 5 in general (359 total attacks) due to the nature of this test, as it was a hackathon with a very tight time limit. This proves that, even if the number of total attempts is important, it is possible to attack a fingerprint sensor in a short time.

### 7.2.1.3 Results per device, per attacker

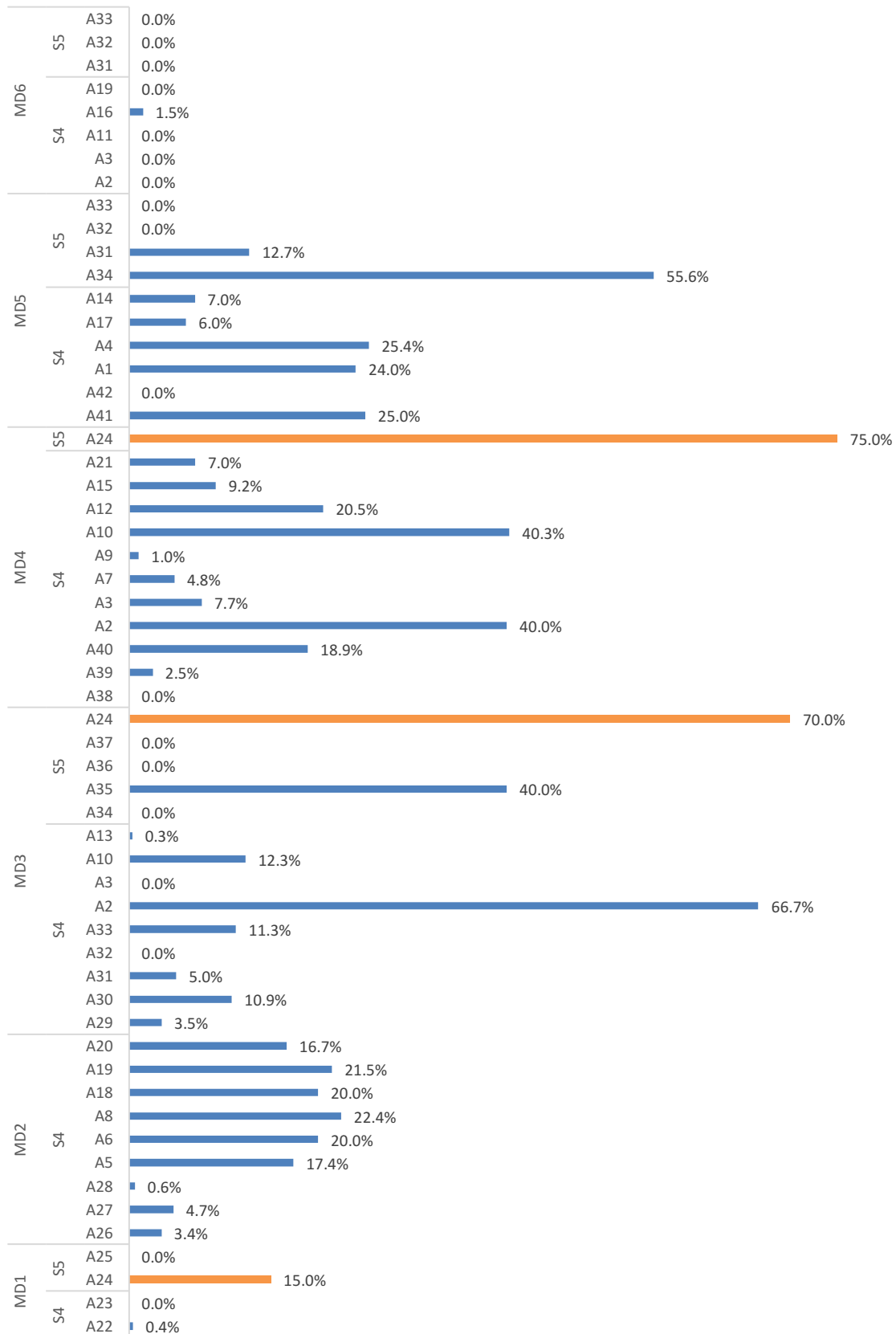
The aim of both experiments was to analyze whether different attackers with the same background and starting point would get similar results. The IAPMR for each mobile device, study and attacker can be seen on Figure 42.

Clearly, it can be confirmed that the results vary highly among attackers, from 0% to 75% successful attacks. 18 out of 46 attackers could not successfully attack the smartphone even once, while *Attacker 24* (study 5, 12-hour limit) obtained an IAPMR of 75%, 70% and 15% on MD4, MD3 and MD1 respectively. *Attacker 2* (study 4) could hack MD3 66.7% of the times and *Attacker 34* (study 5) could do so with MD5 55.6% of the times. Moreover, all attackers had a hard time attacking MD6, as most of them failed except for *Attacker 16* (study 4), who obtained a small IAPMR of 1.5%.

It must be noted that, for study 4, attacks were performed in an ordered way following an evaluation protocol, while for study 5 participants were trying different materials on a tight time limit. This means that a very small number of attacks were attempted on the hackathon. Thus, it is important to visualize the number of total attempts performed by each attacker (Figure 43). It can be observed that, while *Attacker 3* (study 4) obtained the highest IAPMR, he or she carried out very few attempts: 90. Meanwhile, *Attacker 10* (study 4) performed a total of 796 attempts.

The most notable outcome of this subsection is that different attackers get very different results, even having the same starting point. At times, a person (experienced or non-experienced) gets the specific trick for attacking a sensor and from then on, most attacks can work. This can be due to practice or sheer luck.

## Evaluation of Presentation Attack Detection under the Context of Common Criteria



**Figure 42. IAPMR results per mobile device, study and attacker.**



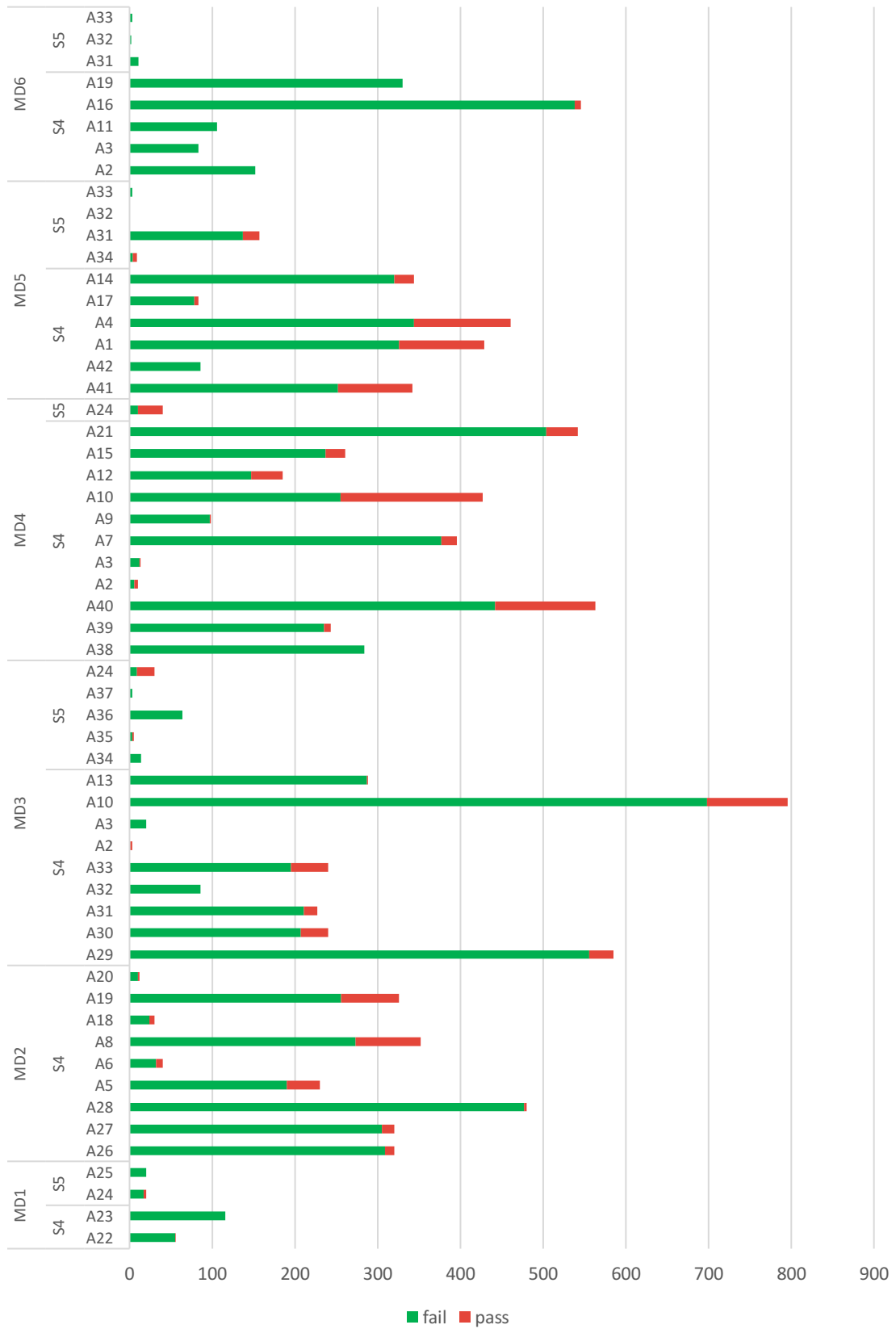
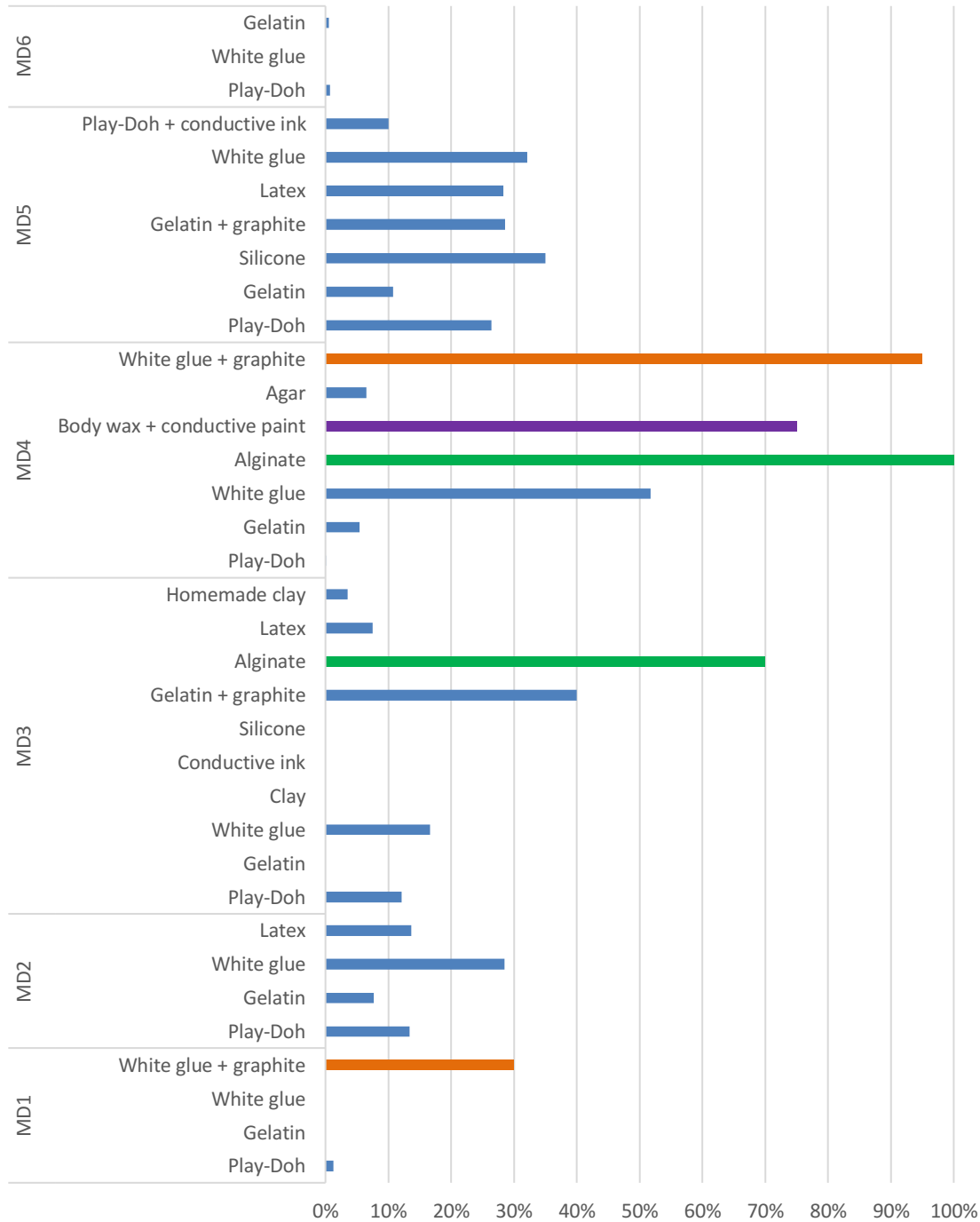


Figure 43. Number of successful (in red) and failed (in green) attacks for each mobile device, divided by study and by attacker.

### 7.2.1.4 Results per device, per PAI species

On each experiment, different materials were used for building the PAIs. On both tests, participants were encouraged to find materials that were successful in attacking smartphone fingerprint sensors. An overview of the results of all PAI species can be seen on Figure 44 and Figure 45.

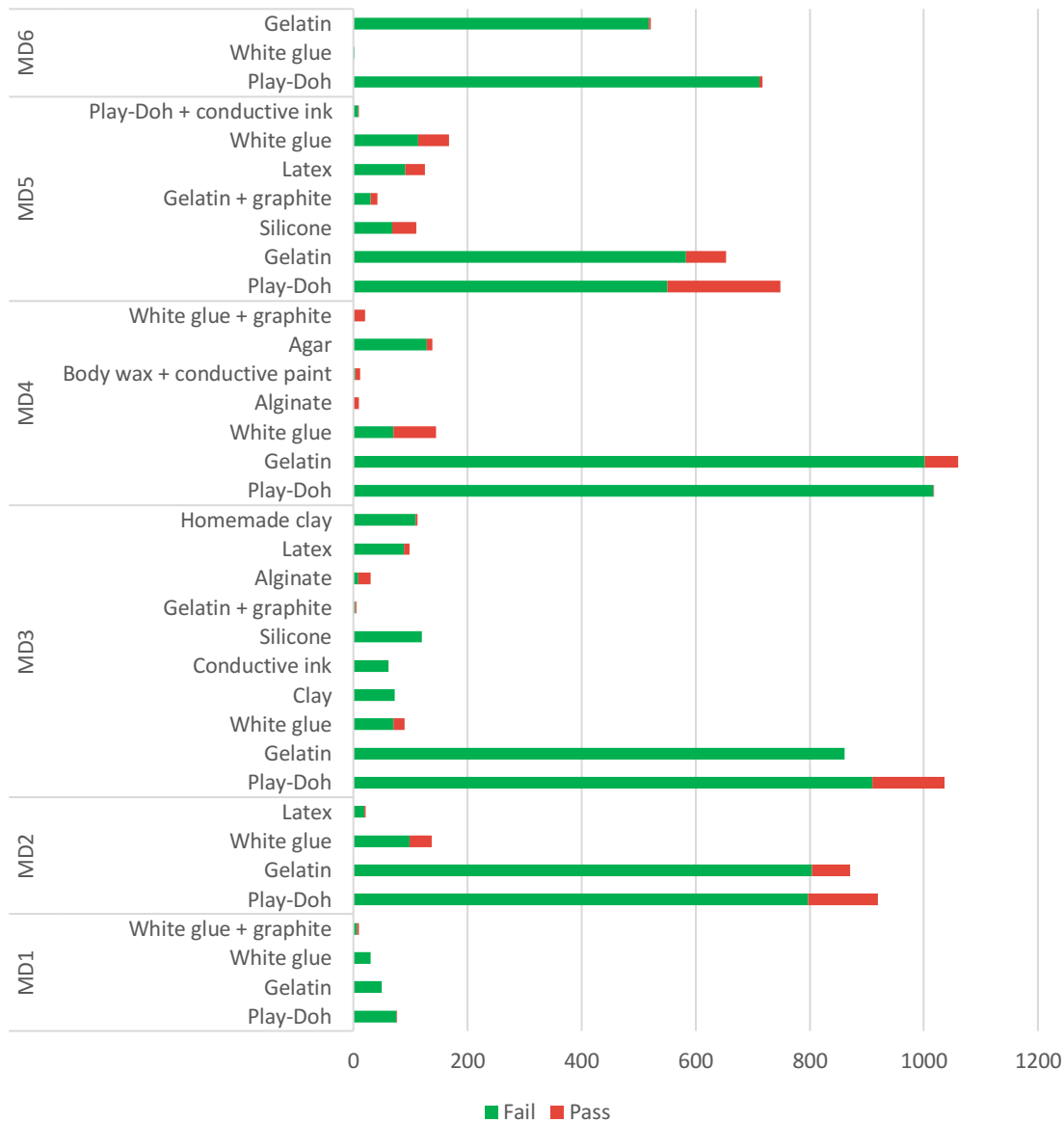


**Figure 44. IAPMR for each PAI species, divided by mobile device (MD1-MD6). The three most successful PAI species are marked in a different color.**

It can be observed that alginate was the most successful PAI species reaching an IAPMR of 100%, followed by white glue with graphite (95%) and body wax with conductive paint on the surface (75%) on third place. The most consistent material within these experiments is Play-Doh, with an IAPMR of 1.6%, 13.4%, 12.2%, 0.1%, 26.4% and 0.7% on devices MD1-MD6, respectively. Nevertheless, alginate and body wax with conductive paint have not been tried on all smartphones. MD3 is the smartphone on which the biggest number of materials has been tried.

Although some materials proved to be very successful on some smartphones, it must be noted again that, very few attempts were performed in comparison with study 4. A graph with the number of passes and fails for each material can be seen on Figure 45. It can be observed that alginate, the PAI species with an IAPMR of 100% for MD4, had very few total attempts (10, all of them performed by the same attacker and with the same finger source).

It must be noted that, for study 4, 46 attackers had 1 week to attack a smartphone while, for study 5, 10 attackers had 12 hours to do so. That is, the subjects for study 4 had 156 more hours for performing the attacks. Interestingly, the average IAPMR is 13.2% and 25.1% for studies 4 and 5, respectively. Thus, in average, those that had a shorter time to carry on the attacks obtained better results. This reinforces the idea that different attackers get very different outcomes and that it is very important to include as many attackers as possible in PAD evaluations.



**Figure 45. Number of successful (in red) and failed (in green) attacks, divided by device and PAI species.**

It is interesting to notice that common spoofing materials like Play-Doh, gelatin and latex do not achieve many successful attacks on MD4, while rarer materials like alginate or body wax with conductive ink do. A similar case happens with MD1: gelatin and latex, very common materials, do not work due to the nature of the technology. As it is a swipe sensor, PAIs broke when trying to use them on the smartphone reader.

### 7.2.2 Vulnerability test results

As it was explained on Section 4.3.1, once all the data has been analyzed after the penetration test, the evaluator shall report which PAI species were successful in attacking each system to report their found vulnerabilities to presentation attacks. The result for these experiments is shown on Table 42.

**Table 42. List of vulnerabilities of smartphones. It must be noted that not all PAI species were tried on every phone and that different numbers of attempts were performed on each experiment.**

PAI species	MD1	MD2	MD3	MD4	MD5	MD6
Play-Doh	x	x	x	x	x	x
Gelatin		x	x	x	x	x
Latex		x				
Silicone					x	
White glue		x	x	x	x	
Latex + graphite						
White glue + graphite						
Gelatin + graphite			x		x	
Alginate			x	x		
Body wax + conductive ink				x		
Gelatin + graphite						
Play-Doh + conductive ink					x	
Homemade clay			x			
Agar				x		

It must be noted that some PAI species were used more times than others. More importantly, not all PAI species were tried on all smartphones by the non-experienced attackers, and most attackers oversaw only one smartphone and not multiple, due to the time constraints.

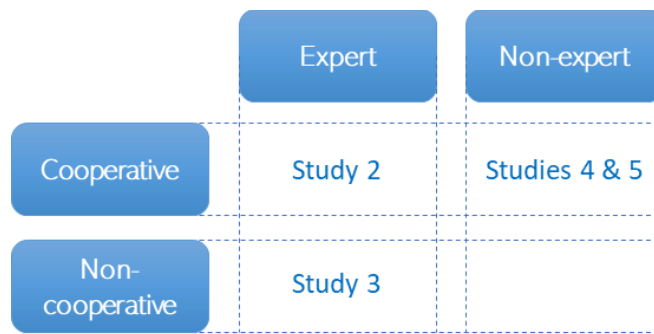
The consequences that may derive from these vulnerabilities are that an attacker could unlock the phone and have access to all the apps that do not require additional security, which are most of them at the time this paper was written.

### 7.3 Comparison with expert attackers

What Chapter 6 and Chapter 7 have in common is that they entail full-system PAD evaluations performed on mobile devices. Chapter 6 gathered two evaluations with an established protocol, carried out by two experts cooperatively and non-cooperatively. On the other hand, Chapter 7 focused on observing the ability of inexperienced attackers to perform cooperative attacks on mobile devices, having a time limit. Although the particular outcomes of each study were detailed in their corresponding chapters, it is also interesting to draw a connection between both, as all of them are about attacking fingerprint sensors embedded in mobile devices. The results that will be compared are per device and study and per attacker.

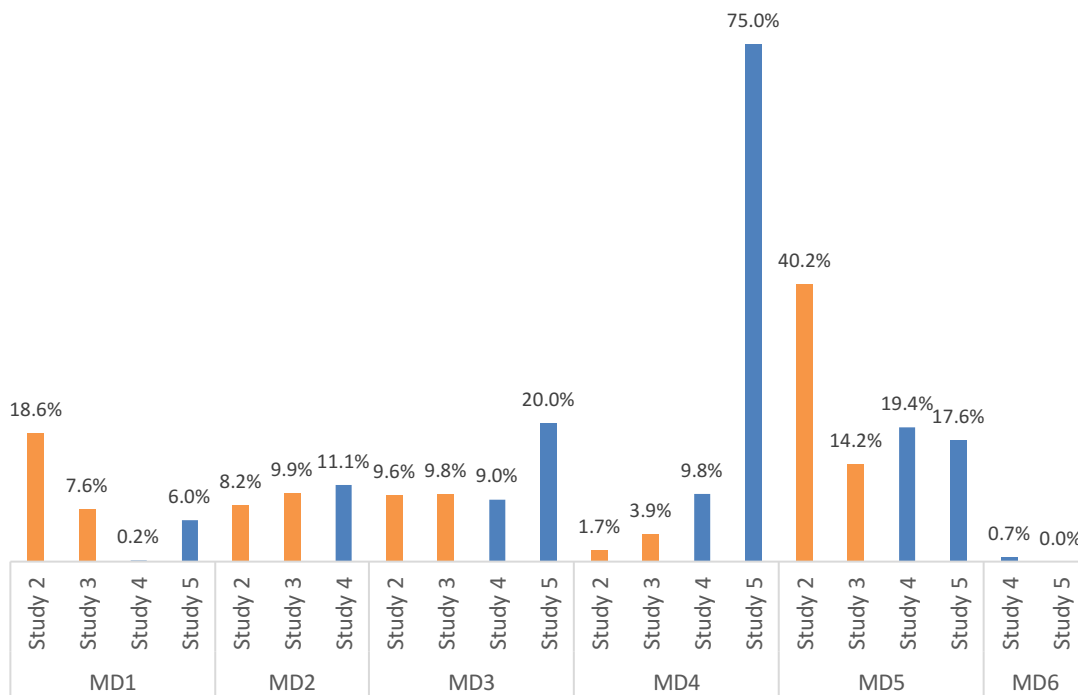
#### 7.3.1 Comparison: results per study

It is interesting to compare the IAPMR results for each study, and mostly for experts and non-experts. It must be reminded that studies 2, 4 and 5 had only cooperative attacks, while study 3 had only non-cooperative ones (Figure 46).



**Figure 46. Characteristics of studies.**

On Figure 47, the total IAPMR for each device and for each study can be observed. It is not clear whether the total of novice attackers perform better or worse than the expert ones: for MD2 and MD3, the results among all studies are very similar; on MD1, experts performed better; on MD4, non-experts obtained considerably better results.

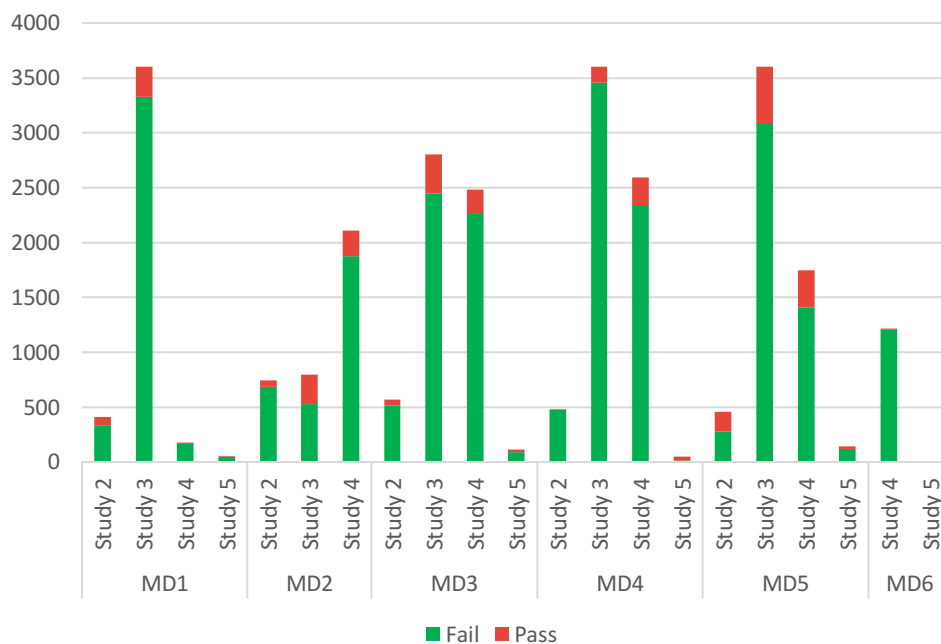


**Figure 47. IAPMR results divided by mobile device and study. The colors correspond to expert/non-expert attackers.**

Nevertheless, once more, it must be noted that as study 5 (hackathon) did not follow an established protocol, very few artefacts were used on the smartphone sensors. Thus, the passes and fails graph must be observed too (Figure 48). In all smartphones except MD6, the expert from study 3 attempted the most attacks, up to 3,600 for some smartphones. Thus, the comparison to be made for the case of study 5 has limitations.

The most outstanding result is the one obtained for MD4 on study 5, achieving very contrasting IAPMRs: 1.7% and 2.9% for expert attackers and 9.8% and 75% for inexperienced ones. As it will be explained on the coming plots, the 75% IAPMR case is due to having used one specific material that proved to be very successful when attacking fingerprint sensors.

On the other hand, MD1 was tricky to use by inexperienced attackers and the number of successful attacks is lower than for the experienced ones. This could be due to the sensor type: being a swipe sensor, it is difficult to avoid the PAI from breaking at the time of use.



**Figure 48. Pass and fail results divided by mobile device and study.**

### 7.3.2 Comparison: results per attacker

This is the key comparison of this subsection: the IAPMR difference among attackers. In general, the results obtained by each experimenter are very different from each other (Figure 49). The IAPMR variability for each mobile device is:

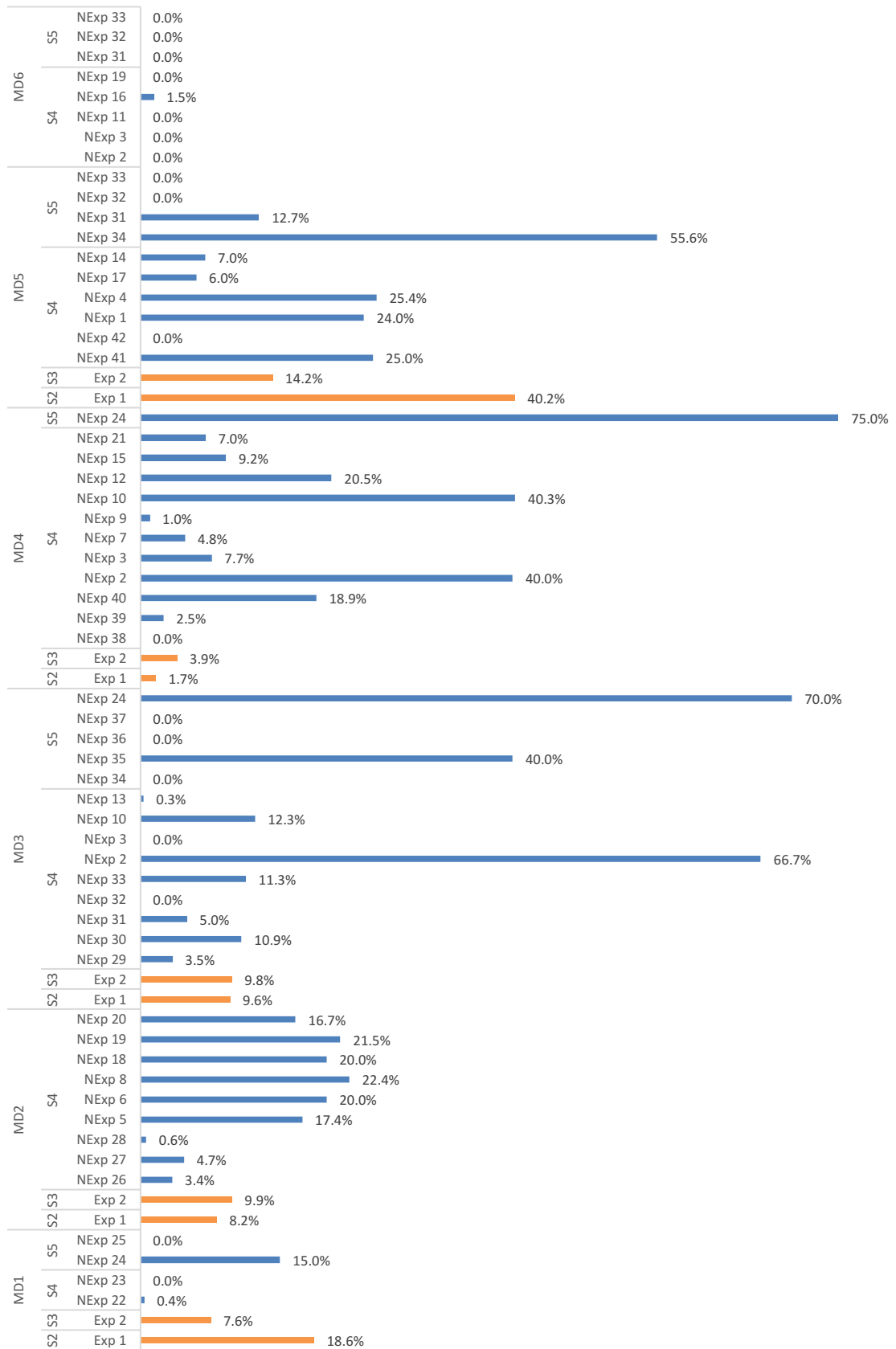
- **MD1:** 0% (NExp 23, 25) - 18.6% (Exp 1)
- **MD2:** 0.6% (NExp 28) – 22.4% (NExp 8)
- **MD3:** 0% (NExp 32, 3, 34, 36, 37) - 70% (NExp 24)
- **MD4:** 0% (NExp 38) - 40.3% (NExp 10)
- **MD5:** 0% (NExp 42, 32, 33) - 55.6% (NExp 34)
- **MD6:** 0% (NExp 2, 3, 11, 19, 31, 32, 33) - 1.5% (NExp 16)

As it can be seen, in 5 out of 6 smartphones, an inexperienced attacker obtained a higher number of successful attacks than the experienced. Nevertheless, the

inexperienced attackers could try a wide range of materials while the experts were limited to the very basic ones of the literature. In the cases where a high IAPMR is obtained, it is usually linked to having used a very successful material for fake finger creation, such as alginate or white glue (as it was seen on the previous section of this chapter). The results by number of passes and fails for each attacker can be found on Figure 50 where again, by far, the expert attacker 2 carried out the highest number of attacks, while the inexperienced attackers made very few attempts in general.



## Presentation Attack Detection evaluation on mobile devices - multiple non-experts



**Figure 49. IAPMR for each attacker, divided by study and device.**

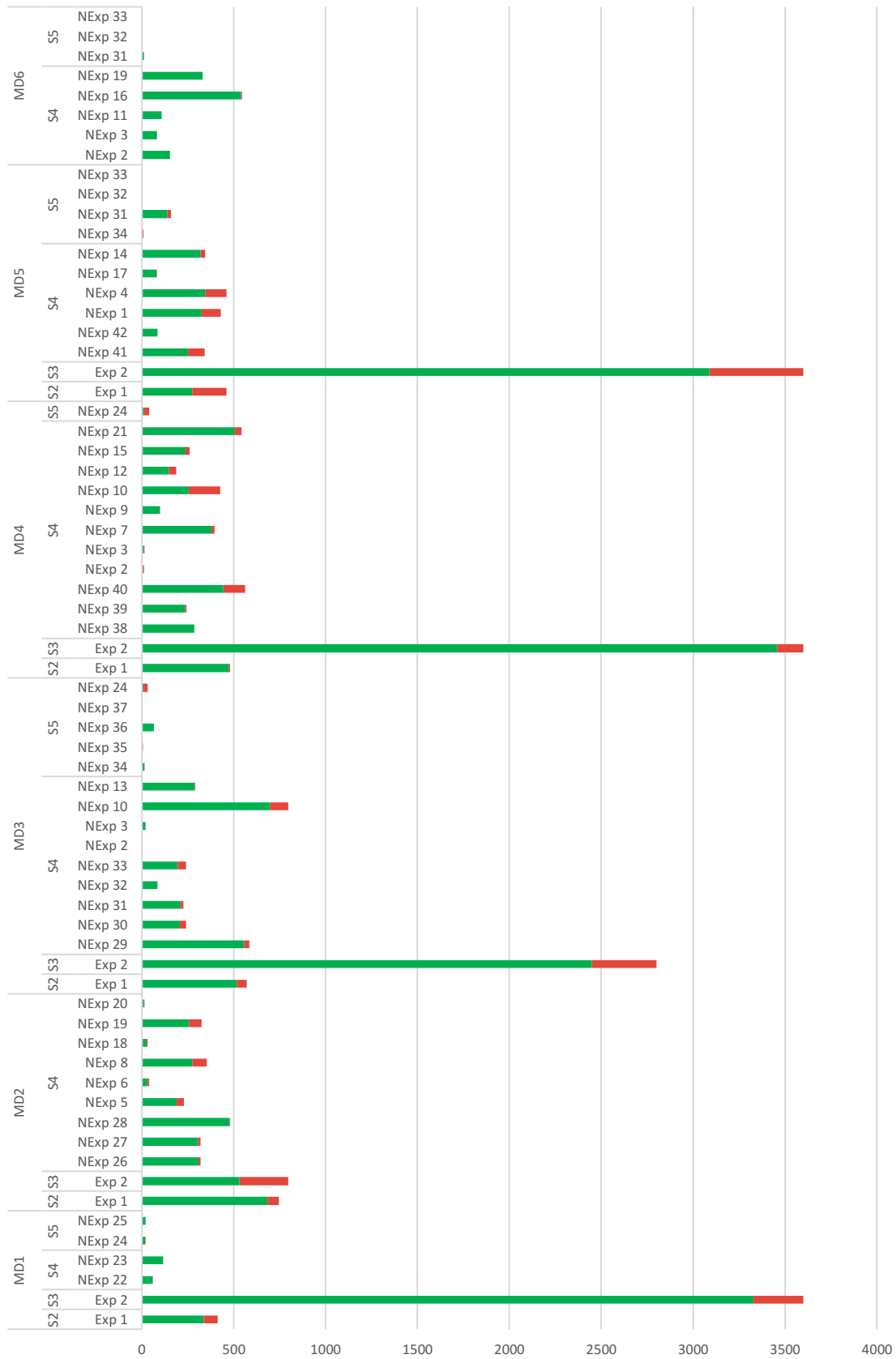


Figure 50. Passes and fails for each attacker, divided by study and mobile device.

## 7.4 Conclusions

In this chapter, 2 experiments were performed on smartphones that have an embedded fingerprint sensor. The aim of both studies was to observe if different attackers obtained different results having the same starting point: a video by an expert creating molds and artefacts and article references. The difference among both tests is that, while for the first one an evaluation protocol was followed and they had one week to perform attacks, for the second one the non-experienced attackers had a tight time limit of 12 hours. Thus, study 5 was only appropriate for finding out which materials proved to successfully attack a smartphone at least once. Throughout the process, some lessons were learnt:

- IAPMR (Impostor Attack Presentation Match Rate) is highly dependent on the evaluator's ability to create artefacts and on the capture subject. Thus, it is important to use as many attackers and capture subjects as possible when evaluating PAD in mobile devices.
- In total, 28 out of 48 attackers (people with no expertise in attacking fingerprint sensors) could successfully attack them within a week and even within 12 hours, just by watching a video of a researcher doing it. Very similar videos are available on YouTube for everyone to see. Nonetheless, these studies have the limitation that each material was not tested on multiple fingers or across multiple users.
- Experience when performing attacks counts sometimes, but anyone can get the trick to a specific reader, either in the first attempt or after months of trials. Every person has very different abilities when attacking a capture device, just as it would happen with cooking.
- Given the large difference in results across different attackers, it is important to include as many attackers as possible in PAD evaluations, the same way it is done with the number of capture subjects. This issue was brought to the standard ISO/IEC 30107-4 and was included in the document.

Nevertheless, it must be noted that even if an attacker can gain access to the smartphone, he or she will not be able to change passwords or add his or her own fingerprint to the system, as a PIN or password is needed for those actions. Moreover, if the attacker finds the smartphone when it's shut down, he or she will also need a PIN or password to unlock it the first time. As a general consideration, it must be noted that including a fingerprint sensor in smartphones greatly increased the security of mobile devices. The reason is that people that had never set up a PIN or password on their phones (due to being uncomfortable or a nuisance) started using the fingerprint reader easily, adding an important layer of protection to their personal phones.

## 7.5 Contributions and dissemination

With these 2 experiments, one journal paper and two conference papers were published. Moreover, several contributions were accepted in the pertinent international standard ISO/IEC 30107-4 Biometric Presentation Attack Detection – Part 4: Profile for evaluation of mobile devices.

### 7.5.1 Journal papers

[95] I. Goicoechea-Telleria, R. Sanchez-Reillo, J. Liu-Jimenez, and R. Blanco-Gonzalo, "Attack Potential Evaluation in Desktop and Smartphone Fingerprint Sensors: Can They Be Attacked by Anyone?," *Hindawi*, vol. 2018, pp. 1–13, 2018.

- Study on non-expert attackers and comparison with other evaluations on fingerprint readers.

### 7.5.2 Conference papers

[98] I. Goicoechea-Telleria, J. Liu-Jimenez, H. Quiros-Sandoval, and R. Sanchez-Reillo, "Analysis of the attack potential in low cost spoofing of fingerprints," *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2017–Octob, pp. 1–6, 2017.

- Study of non-expert attackers and comparison with one expert.

[99] R. B. Gonzalo, B. Corsetti, A. Hussein, and I. Goicoechea-Telleria, "Attacking a smartphone biometric fingerprint system : a novice's approach," *2018 Int. Carnahan Conf. Secur. Technol.*, vol. 675087, no. October, pp. 1–5, 2018.

- Report of the hackathon experiment.

### 7.5.3 Standardization

[2] SC 37, "ISO/IEC 2nd WD 30107-4 Biometric presentation attack detection - Part 4: Profile for evaluation of mobile devices," 2018.

- Added that having multiple attackers perform the same test is as important as having multiple capture subjects, using these studies as proof.

## Chapter 8. Detection of Presentation Attacks

---

AS IT WAS detailed on Section 3.3 *Presentation attack detection mechanisms*, extensive research has been carried out in the literature in order to detect fingerprint attacks at the presentation level. Once several desktop and mobile device fingerprint sensor vulnerabilities were evaluated, it was decided to create a new method to overcome presentation attacks. The chosen approach focuses on optical readers, generally used at border controls and increased security scenarios. As it was noted on the same chapter, hardware solutions usually reach better error rates than the software ones, because more information of the fingerprint can be obtained if the PAD mechanism is part of the capture process design than analyzing the images *posteriori*.

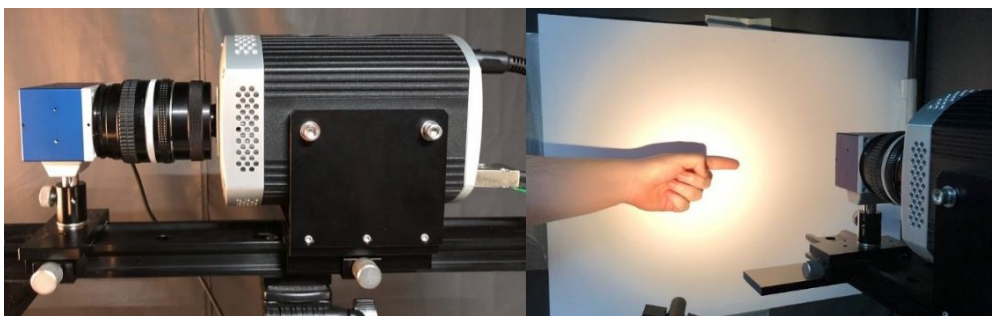
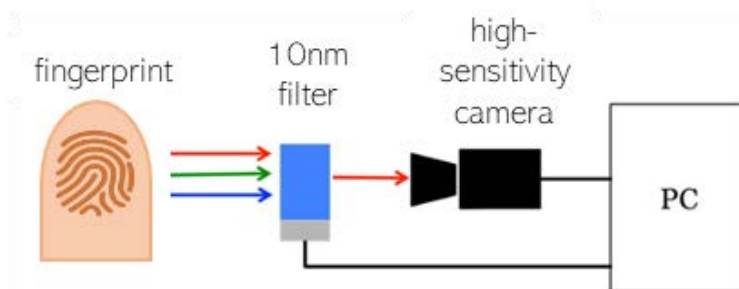
Two approaches were tested based on the distinctiveness of skin features under different wavelength illumination. First, a narrow-band camera with 10nm wavelength increments was used to analyze a small database of real and fake fingerprints and observe the differences in characteristics. Second, portable microscopes with special lighting conditions were used to do the same experiment but gathering a bigger database. These solutions are compatible with optical sensors. However, because of their bulkiness, they are not compatible with other readers, such as capacitive ones. The image processing and classification algorithms were very similar for both studies. More details will be given on the following subsections.

## 8.1 Narrow-band camera

The goal of this study is to use a narrow-band camera's advantages to observe a fingerprint in 10nm wavelength increments and to classify bona fide and attack attempts using Bag of Features. All results are given in accordance to the standard on Presentation Attack Detection ISO/IEC 30107-3.

### 8.1.1 Methodology and image capture

All real fingerprints and artefacts were captured with a multiband camera. The setup (Figure 51) was the same used for the experiment on [100], where they explored the number of hand features obtainable in different wavelengths. The outcome of that study was that, at certain bands, a bigger number of characteristics could be obtained when capturing a human hand and chicken livers. Thus, the idea for this study was to use the same approach with real and fake fingers, in order to observe which bands gave more distinctiveness for image classification algorithms. The setup is a VariSpec™ liquid crystal tunable filter (CRi) as a controllable narrow-band filter in increments of 10nm over a range of 400–720nm. To overcome the low light intensity during filtering, an optiMOS camera (QImaging) was used with a high-sensitivity image sensor with a resolution of 1920 × 1080 pixels. The maximum frame rate is of 100 fps. The light source was an LP-500U white LED manufactured by FalconEyes.



**Figure 51. Setup of the narrow-band camera and bona fide subject holding finger ready for capture.**

As shown on Figure 51, the subject holds his or her finger on the wall and the narrow-band camera captures 36 wavelengths in one take, from 400 to 720nm plus R, G and B.

The setup of the camera belonged to a hospital laboratory, and thus we only had a very narrow window of access to the system. Hence, only one visit was done per capture

subject and only 3 subjects could access the laboratory. In total, 9,646 images were obtained. The details of the captured database can be found on Table 43. The selection of PAI species was Play-Doh (most common material used in studies due to its ease of use and obtention), latex (transparency and resemblance to a real finger) and transparent nail polish (similar to latex, but possible to get a very thin layer that can be easily hidden from oversight). Fingers were captured in two different conditions each: normal and with hand cream. This is because some real fingers with moisturizer on the surface could confuse a PAD mechanism with a fake finger.

**Table 43. Details of the database following requirements of ISO/IEC 30107-3.**

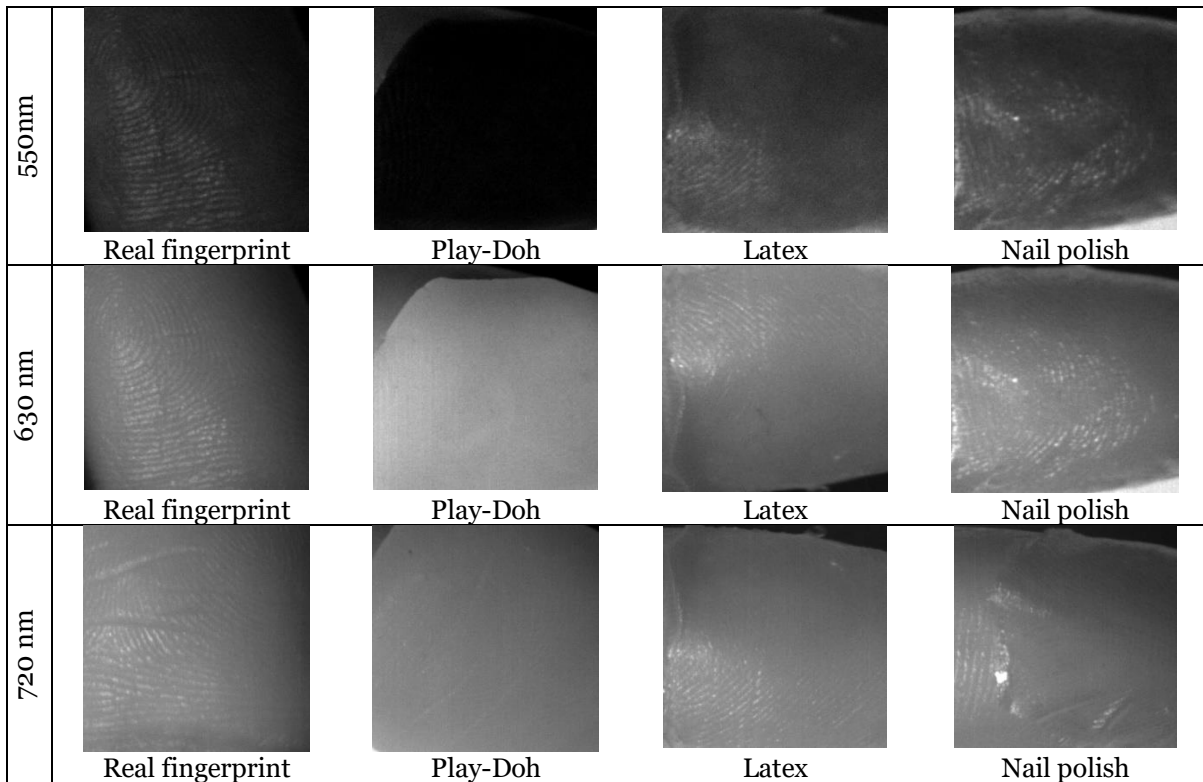
<b>Presentation attack instruments</b>	18
<b>PAI species</b>	3 (Play-Doh, latex, transparent nail polish)
<b>PAI series</b>	1 per source
<b>Visits</b>	1
<b>Test subjects</b>	3
<b>Artefacts per test subject</b>	6 (thumb, index and middle fingers)
<b>Sources</b>	18
<b>PAI species</b>	3 (Play-Doh, latex, transparent nail polish)
<b>Bona fide finger conditions</b>	2 (normal, hand cream)
<b>Output information from PAD mechanism</b>	PAD score
<b>Attempts per presentation</b>	3
<b>Attack attempts</b>	162 (per wavelength)
	5,832 (total)
<b>Bona fide attempts</b>	98 (per wavelength)
	3,814 (total)
<b>Images collected</b>	260 (per wavelength)
	9,646 (total)
<b>Wavelengths</b>	36 (33 narrow-band and R, G and B)

### 8.1.2 Wavelength observations

After the capture, some appreciations were made on the different observable characteristics of fingerprints and artefacts:

- 400-450nm: Noisy images, no fingerprints can be seen.
- 460nm: first noticeable fingerprint.
- 530-580nm: patches on the fingerprint.
- 580-590nm: Play-Doh artefacts are very dark.
- 600nm: fingerprints and artefacts change from dark to bright.
- 610nm: noticeable veins. Play-Doh is very bright.
- 630nm: wrinkles are not noticeable anymore.
- 670nm: very bright fingerprints.
- 690nm: sweat is more perceivable.

A few examples of captured images can be seen on Figure 52. It is apparent that Play-Doh has very distinct characteristics when observed at different wavelengths. This will make this PAI species easily classifiable.



**Figure 52. Examples of real and artefact samples at 550nm and 630nm.**

### 8.1.3 Processing and classification

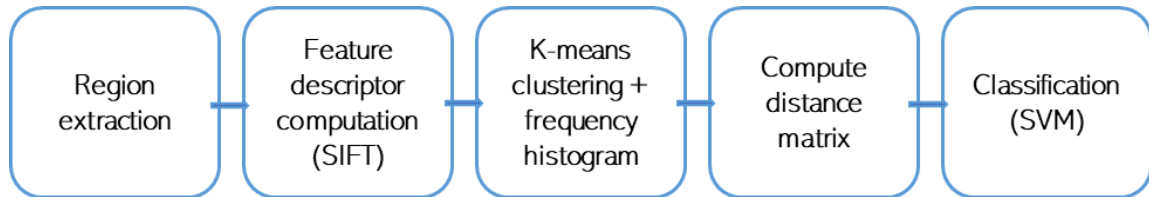
Two different approaches were used for the processing of the images:

- Wavelength study and selection: no preprocessing was needed for this approach. Further details will be explained on Section 8.1.4.
- Image alignment and subtraction: based on the experiment where the same camera was used to obtain features [100], the three most relevant wavelengths were chosen for the processing (530nm, 610nm and 720nm). As images from different wavelengths are taken at slightly different times, first an alignment was done, and then the three images were combined into one by subtraction and addition (the 610nm image was subtracted from the 720nm image, and then the 530nm sample was added).

Once the images were processed and prepared, the classification was performed. In both cases, the approach used for classification is *Bag of Features* or *Bag of Visual Words*. This model, initially used for document classification known as *Bag of Words*, can also be suitable for fingerprint image classification. This is because it does a good job distinguishing textures by creating frequency distributions of image patches, as it is a vector of occurrence count of a vocabulary of local image features (Figure 53). Thus, it was thought to be adequate for this case, as differences in textures could indicate if a finger is real or fake.



The model uses SIFT feature descriptors, appropriate for this case because they handle well intensity, rotation and scale differences. Then, these vector-represented patches are sorted into “codewords”, which in turn convert into a “codebook”. For this, k-means clustering is performed automatically and the codewords are defined as the centers of these clusters. This way, each image patch is mapped to a specific codeword and any image fed to the algorithm can be represented by a frequency histogram of codewords [101]–[103]. Once clusters and distance matrices are computed, the classification is performed using support vector machines (SVM).



**Figure 53. Bag of Features or Bag of Visual Words diagram.**

#### 8.1.4 Results

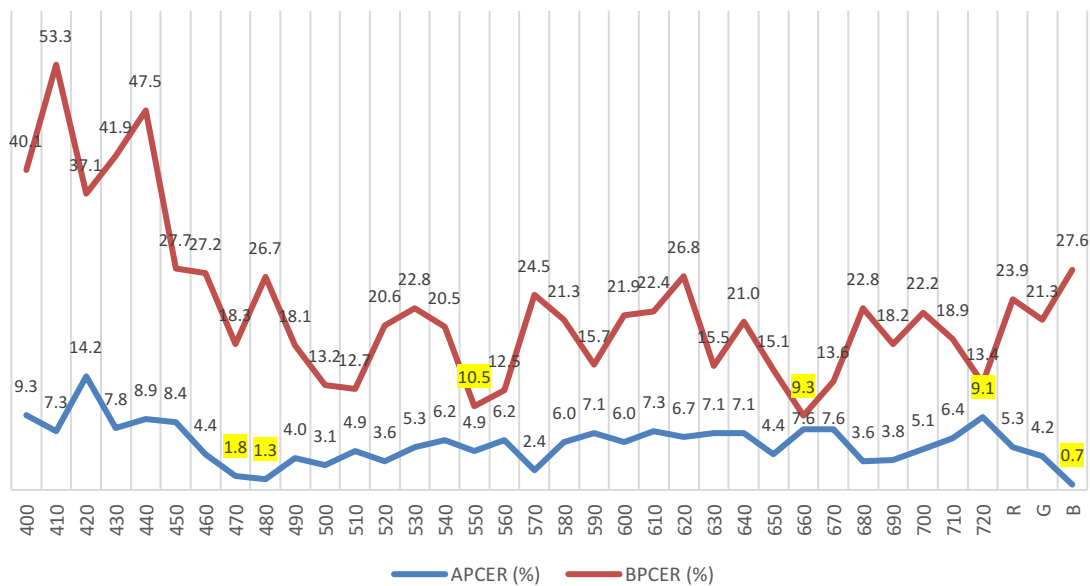
The results will be given according to ISO/IEC 30107-3 requirements. In this case, it is a PAD subsystem, so the relevant metrics are APCER (proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario) and BPCER (proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario). These were addressed in Section 2.3.2.

##### 8.1.4.1 Selected wavelengths study

The goal of this study is to use the narrow-band camera’s advantages to see a fingerprint in increments of 10nm and discern which wavelengths are more useful for classification. Thus, in this case, all wavelengths were used separately to train the algorithm. As a result, APCER and BPCER values for each wavelength are shown on Table 44 and a plot is shown on Figure 54 for clarification.

**Table 44. APCER and BPCER values for each wavelength (increments of 10nm and RGB). 70% training, 30% testing.**

Wavelength (nm)	APCER (%)	BPCER (%)	Wavelength (nm)	APCER (%)	BPCER (%)
400	9.3	40.1	580	6.0	21.3
410	7.3	53.3	590	7.1	15.7
420	14.2	37.1	600	6.0	21.9
430	7.8	41.9	610	7.3	22.4
440	8.9	47.5	620	6.7	26.8
450	8.4	27.7	630	7.1	15.5
460	4.4	27.2	640	7.1	21.0
470	1.8	18.3	650	4.4	15.1
480	1.3	26.7	660	7.6	9.3
490	4.0	18.1	670	7.6	13.6
500	3.1	13.2	680	3.6	22.8
510	4.9	12.7	690	3.8	18.2
520	3.6	20.6	700	5.1	22.2
530	5.3	22.8	710	6.4	18.9
540	6.2	20.5	720	9.1	13.4
550	4.9	10.5	R	5.3	23.9
560	6.2	12.5	B	4.2	21.3
570	2.4	24.5	G	0.7	27.6



**Figure 54. APCER and BPCER for each wavelength. The three lowest results for APCER and BPCER are marked in yellow.**

As it can be seen, the 10 wavelengths that showed to reach a better average APCER and BPCER at classification are 470, 490, 500, 510, 550, 560, 650, 660, 670 and 690nm. Thus, it was decided to use all these wavelengths for another analysis by using all of them together for training. In total, 980 bona fide and 1,620 attack images were used. As for every other case, each result was calculated 20 times and then averaged,

and all samples were randomized before each iteration. A cross validation of the results obtained using this technique can be seen on Table 45.

**Table 45. Cross validation of APCER and BPCER results for the selected wavelengths study. All values were calculated 20 times and then averaged.**

	Training percentage				
	10%	30%	50%	70%	90%
<b>APCER</b>	4.99	7.01	5.76	3.89	4.83
<b>BPCER</b>	55.32	27.21	21.97	17.55	10.47

#### 8.1.4.2 Image alignment and subtraction study

As said on 8.1.3, images from three different wavelengths (530nm, 610nm and 720nm) are aligned and combined by addition and subtraction, and then are classified by using Bag of Features. The APCER and BPCER results are shown on Table 46 depending on the training percentage used for classification, from 10% to 90%. As it can be seen, the classification results are better for attack classification than for bona fide classification.

**Table 46. Cross validation of APCER and BPCER results for the image alignment and subtraction study. All values were calculated 20 times and then averaged**

	Training percentage				
	10%	30%	50%	70%	90%
<b>APCER</b>	4.62	4.66	1.98	3.67	7.5
<b>BPCER</b>	45.05	26.86	18.17	9.94	8.86

The results to be compared are total APCER and BPCER of both studies, as other intermediary APCER and BPCER results have too few samples (that is, results by PAI species and results by capture subject). Taking the 50% training result from the cross validations, the image combination approach gets an APCER of 1.98% and a BPCER of 18.17%, while the selected wavelengths approach obtains a 5.76% APCER and 21.97% BPCER. Although results for bona fide samples are poor, the error rate for misclassifying attacks is low compared to other approaches of the literature.

#### 8.1.5 Conclusions

A study was performed with a multiband narrow-band camera to observe fingerprints in increments of 10nm and choose the best wavelengths for classification. Two approaches were used prior to classification: 3 wavelength combination by addition and subtraction, and best wavelength selection. The classification was done using Bag of Features. Some lessons were learned from this work:

- It is important to study fingerprints in narrowly separated wavelengths, as different features and characteristics can be obtained for each. Also, some wavelengths give significantly better results than others.
- In this case, combining several wavelengths in a single image worked better than training the algorithm with mixed wavelengths.

- Bag of Features gives good results for fingerprint attack classification, as it is designed for distinguishing textures regardless of position and orientation.

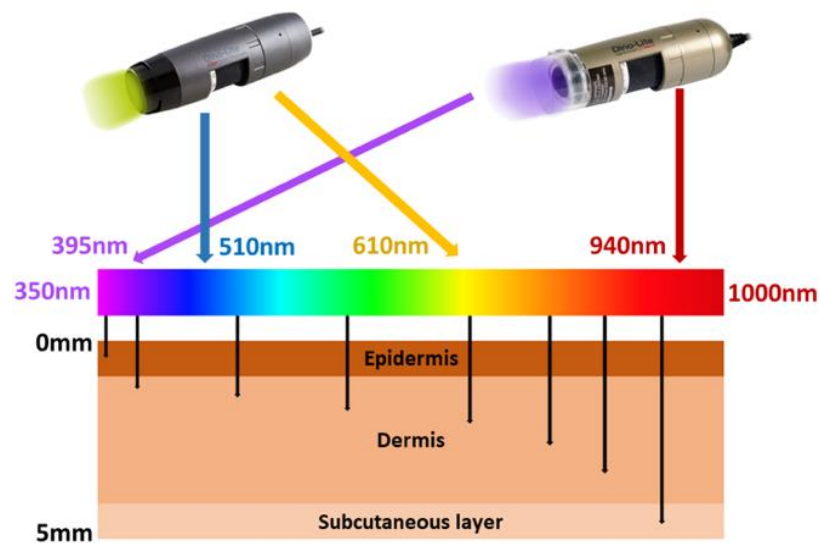
## 8.2 Microscopes with special lighting

Once the previous short experiment was performed, it was seen that observing fingerprints in different wavelengths can have promising outcomes, even more when combined with the Bag of Features classification algorithm. Nevertheless, the solution was too bulky, so it was decided to look for a more portable system that would follow the same approach of illuminating fingerprints in different lighting conditions. Also, another goal was for this solution to be cost-effective.

For that end, 2 handheld microscopes with special lighting were found and a PAD evaluation was developed and performed. In total, 7,704 images of fake and real fingerprints of 17 subjects were captured. These images were processed and classified using Bag of Features algorithms (as in the previous experiment), obtaining an APCER of 1.78% and a BPCER of 1.33% at 70% training samples (3.99% and 1.11% for 50% training, respectively). It must be noted that these results were obtained even including a capture subject with non-conformant fingerprints (no ridges or valleys) in the database. Moreover, no fingerprint samples were left out, minus those that were the evaluator's fault – wrong finger, wrong LED wavelength turned on. All results are given in accordance to the standard on Presentation Attack Detection ISO/IEC 30107-3.

### 8.2.1 Methodology and image capture

According to several works on fingerprint and skin imaging [100], [104]–[106], different features of the skin can be observed at different wavelengths, depending on the penetration of the light, and thus, on the wavelength used. For this reason, it was decided to use two special lighting microscopes: Dino-Lite AD4113T-I2V (UV and IR lights, 395nm and 940nm respectively) and Dino-Lite Edge AM4115T-GRFBY (fluorescent lighting, excitation at 480nm and 575nm and emission at 510nm and 610nm). The cost of these microscopes was less than 500€ and less than 1000€ respectively at the time of writing, but after the study it will be concluded that a cheaper solution is possible, as only one excitation and one emission wavelength will be needed. As it is usually the case, the solutions used during research stages are more expensive than the final commercial solution. Once the study is made, a simpler, cheaper system can be developed by a manufacturer, as for the final product less microscope amplification and less wavelengths will be needed for obtaining the results. That is why it is viable to include this solution in commercial optical fingerprint devices. An overview of the skin penetration of each wavelength can be seen on Figure 55.



**Figure 55. Different skin penetration levels depending on wavelength of digital microscopes.**

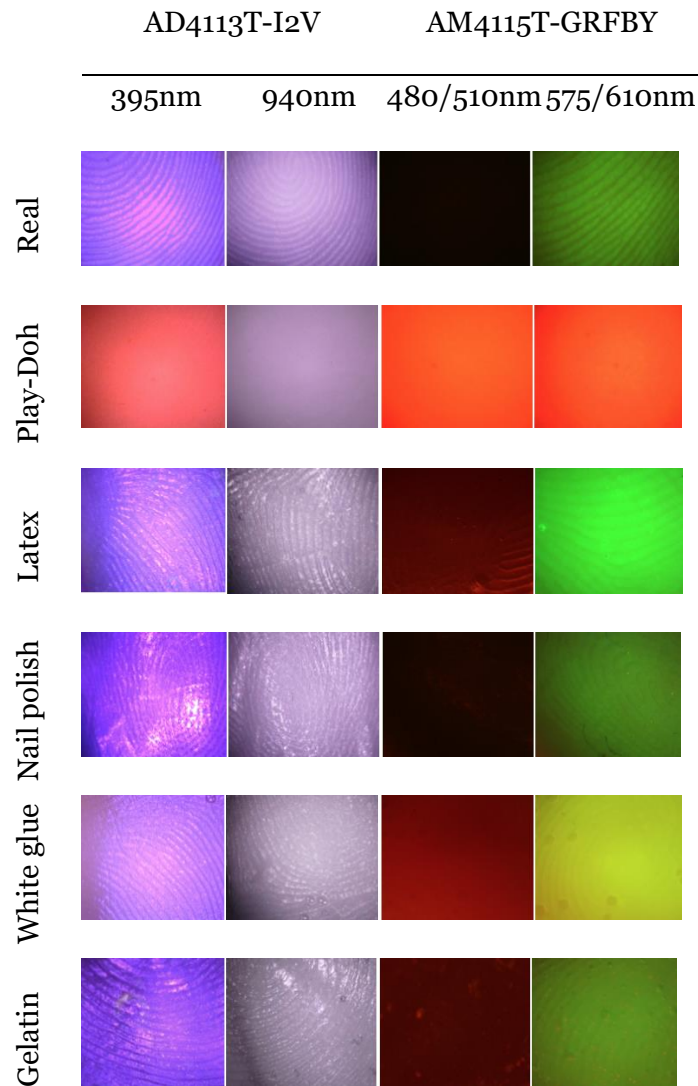
A PAD evaluation was carried out with the microscopes, in order to test how well this technique performs in detecting artefacts. As with the rest of experiments in this Thesis, Common Criteria [18] and ISO/IEC 30107-3 [1] standards were followed.

As a reminder, the evaluator is not expected to determine the exploitability for potential vulnerabilities beyond those for which a Basic attack potential is required to effect an attack. That is, once a fake finger material with a Basic attack potential has proven to be successful, no attacks that would require a higher difficulty should be made, because the system is already confirmed to be vulnerable to easier attacks. Taking this in to account for the experiment, the easiest attacks were performed by using readily available and low-cost materials for building fake fingers. A test was designed following procedures from the Standard ISO/IEC 30107-3 [1] and its details can be seen on Table 47. As a note, in this case more PAIs and more capture subjects were used in comparison with the previous test with the narrow-band camera, as the first experiment was performed only as a proof of concept that needed to be expanded in the future.

**Table 47. Details of the database following requirements of ISO/IEC 30107-3.**

<b>Presentation attack instruments (PAI)</b>	438 (96 Play-Doh, 84 latex, 84 gelatin, 84 white glue, 90 nail polish)
<b>PAI species</b>	5 (Play-Doh, latex, transparent nail polish, gelatin, white glue)
<b>PAI series</b>	1 per source
<b>Visits</b>	2 per bona fide 1 per PAI species
<b>Capture subjects</b>	17 (13 asian, 3 caucasian, 1 african)
<b>Artefacts per capture subject</b>	6
<b>Sources</b>	96 fingers
<b>Output PAD information</b>	PAD score
<b>Attempts per presentation</b>	3
<b>Wavelengths</b>	4
<b>Attack attempts</b>	1,314 (per wavelength)
	<b>5,256 (total)</b>
<b>Bona fide attempts</b>	612 (per wavelength)
	<b>2,448 (total)</b>
<b>Images collected</b>	1,923 (per wavelength)
	<b>7,704 (total)</b>
<b>Attacker's expertise</b>	Expert (by the definition of CC's attack potential [18])

A Matlab capture tool was developed to obtain images of fingerprints in an automated manner. It lets the evaluator enter bona fide and attacker IDs, number of attempts per finger, visit number, image resolution, whether they are real/artefact fingers, gender, PAI species, wavelengths and fingers. The app opens a window to visualize the microscope image output and captures the images in a sequence depending on the chosen parameters. As expected, different lighting conditions gave out different features when inspecting fingerprint images. Examples of images in different wavelengths are shown on Figure 56.



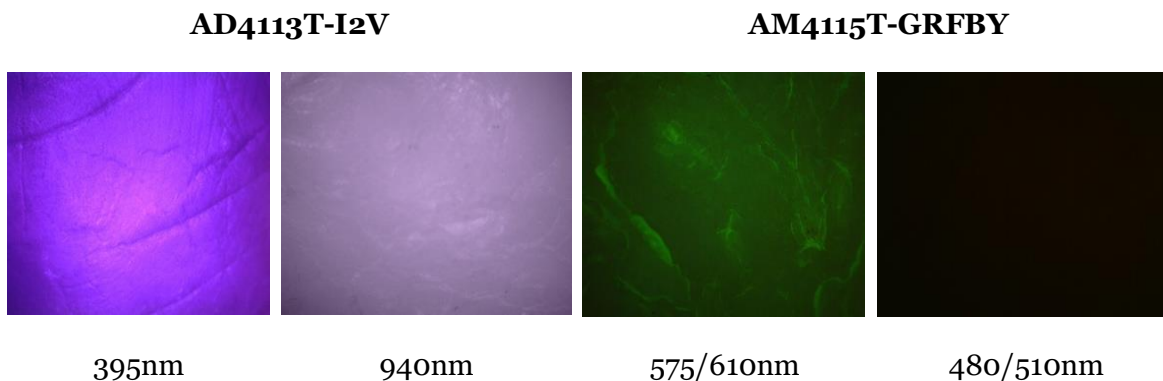
**Figure 56. Examples of real and PAI images captured in different wavelengths.**

As it can be observed, the outputs can be easily distinguished in some cases. Play-Doh, the most common material used for spoofing, has very different features in every wavelength, so it can be easily detected (smoother or no edges, different color). Latex, nail polish and gelatin artefacts have sharper edges (mostly in UV and IR wavelengths). White glue has very clear bubbles on the 575/610nm wavelength, no matter how carefully the artefact is created (they cannot be seen with a naked eye).

### 8.2.1.1 Fingerprints with special characteristics

Commonly, in evaluations found in the literature, fingerprints with special characteristics are discarded from the test. In this work, we chose to be inclusive and execute a realistic study, so a subject with fingerprints with special characteristics was included. This user presented non-conformant fingerprints due to a skin disease, meaning that they did not have any ridges or valleys, so they would be deemed unfit for recognition. On Section 8.2.3.5, we calculate results both including and excluding this subject with the goal of measuring the impact of non-conformant fingerprints in

realistic situations. As it can be seen on Figure 57, ridges and valleys are barely noticeable, if not at all.



**Figure 57. Examples of non-conformant fingerprints of one user of the database with a skin disease, in different wavelengths.**

### 8.2.2 Processing and classification

For this work, no preprocessing or cropping was necessary before feeding the images to the chosen model, Bag of Features. As it was seen on the previous experiment, this algorithm does a good job distinguishing textures, and thus it works well with fingerprint classification. More details were explained on 8.1.3.

The results were calculated 10 times each and averaged and a cross-comparison was done with training at 10%, 30%, 50%, 70% and 90% of samples (randomized by capture subject, and never including the same subject both for training and testing). The vocabulary size of Bag of Features was 850, 80% of the strongest features were used and the grid step was of 16x16. In order to avoid adjusting parameters for only this specific database, these parameters were chosen with only the first few captured samples. Then, once the database capture was completed, the algorithm was applied without changing the parameters and they still performed well. In all cases, the subjects used for training were not used for testing. Two tests were made for classification: separate wavelengths and separate wavelength and channel. This way, it could be seen which wavelengths and channels behaved best for performance.

### 8.2.3 Results

This section gathers the results obtained in different tests, showing the classification error rates APCER and BPCER, as explained on 2.3.2. The tests performed are: classifying each wavelength separately, classifying each wavelength and RGB channel separately, using only the red channel of the 575/610nm wavelength and, lastly, leaving out the non-conformant samples of one capture subject (as it was explained in previous sections).

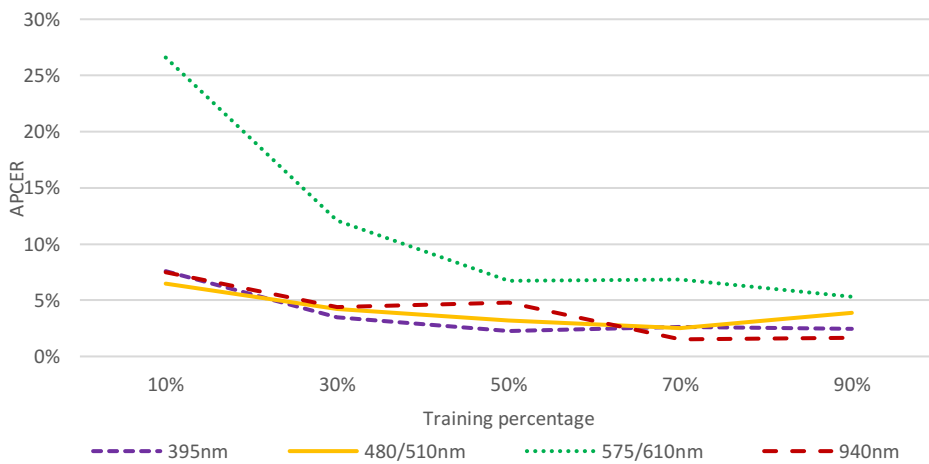
#### 8.2.3.1 By wavelength

This subsection shows the results of classifying each wavelength separately. Each microscope has two different lighting modes:

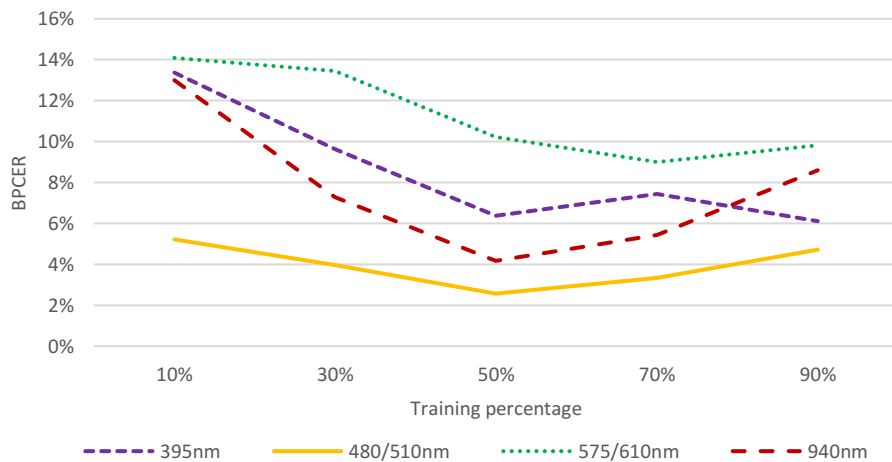


- Dino-Lite AD4113T-I2V:
  1. UV (395nm)
  2. IR (940nm)
- Dino-Lite AM4115T-GRFBY: fluorescent lights.
  1. Excitation at 480nm and emission at 510nm
  2. Excitation at 575nm and emission at 610nm

Thus, each mode was studied separately. The samples were fed in RGB to the algorithm, and it converts them to grayscale before classification. The database includes non-conformant samples from a subject with a skin disease. Results for APCER and BPCER cross-comparisons can be seen on Figure 58 and Figure 59, respectively.



**Figure 58. APCER cross-comparison results for each lighting mode. Every result was calculated 10 times and then averaged.**

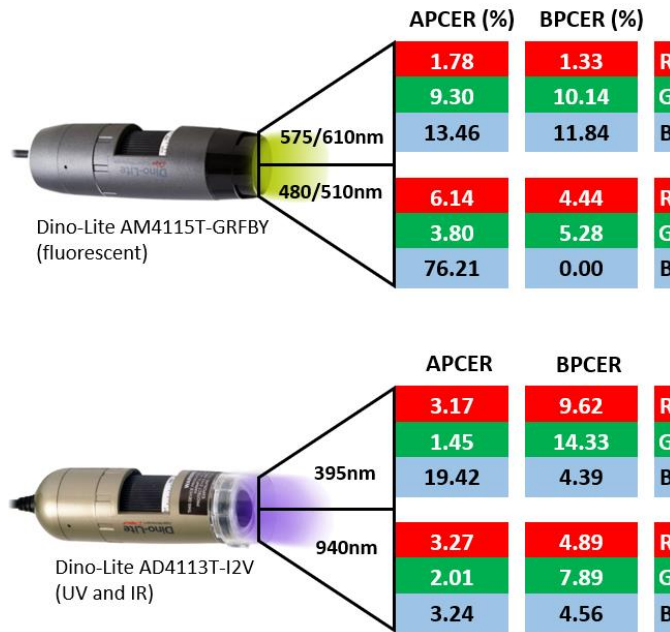


**Figure 59. BPCER cross-comparison results for each lighting mode. Every result was calculated 10 times and then averaged.**

It can be observed that some wavelengths perform better than others. 395nm and 480/510nm seem to work better for APCER results but, for the BPCER case, 480/510nm and 940nm yield a lower error rate.

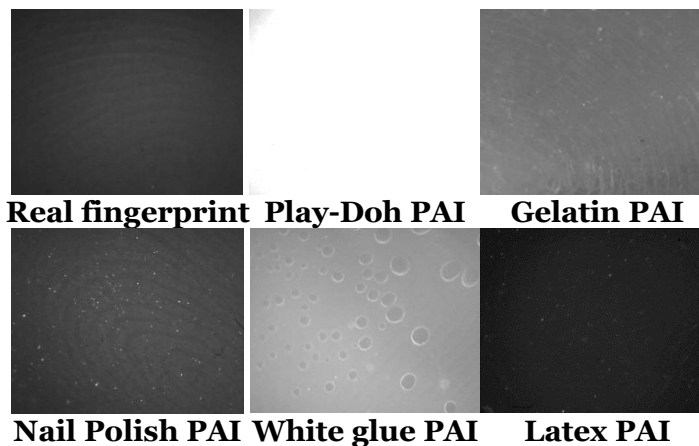
### 8.2.3.2 By wavelength and channel

It was decided to break down the tests also by RGB channels, to check if some perform better than others. Results of this are detailed on Figure 60.



**Figure 60. APCER and BPCER results separated by wavelength and channel. 70% training, 30% testing.**

This study shows that the best performing conditions are using the red channel of the 575/610nm mode, one of the available lightings of the fluorescent microscope. With a naked eye, it can be observed that there are indeed perceivable differences (Figure 61).



**Figure 61. Noticeable variation in R channel.**

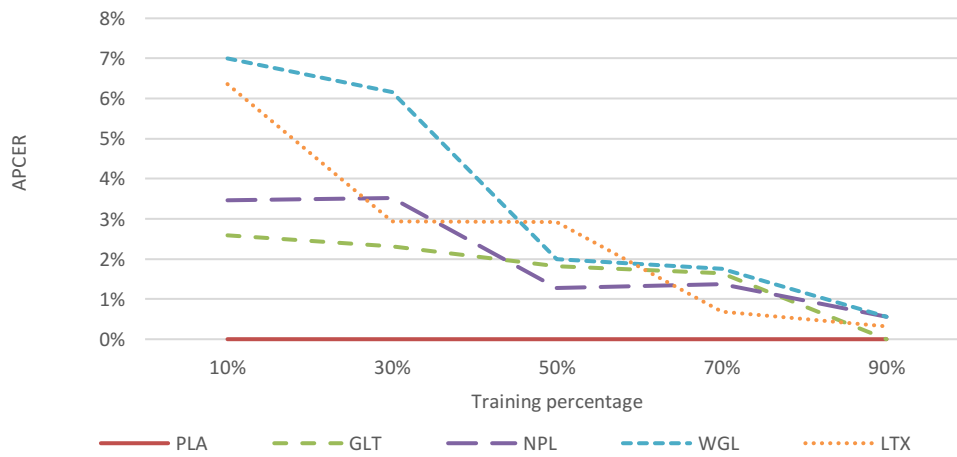
Interestingly, using the 480/510nm in the blue channel, the BPCER is always 0% on this database. It was calculated 30 times. Thus, if wanted, only this channel could be used for eradicating the BPCER error of classifying real fingers as attacks. Nevertheless, this channel is the least suitable for APCER, as the error is very high

(76%). As the 575/610nm wavelength in the red channel seems to achieve lower error rates, a full cross-comparison was performed with it and it can be seen on Table 48.

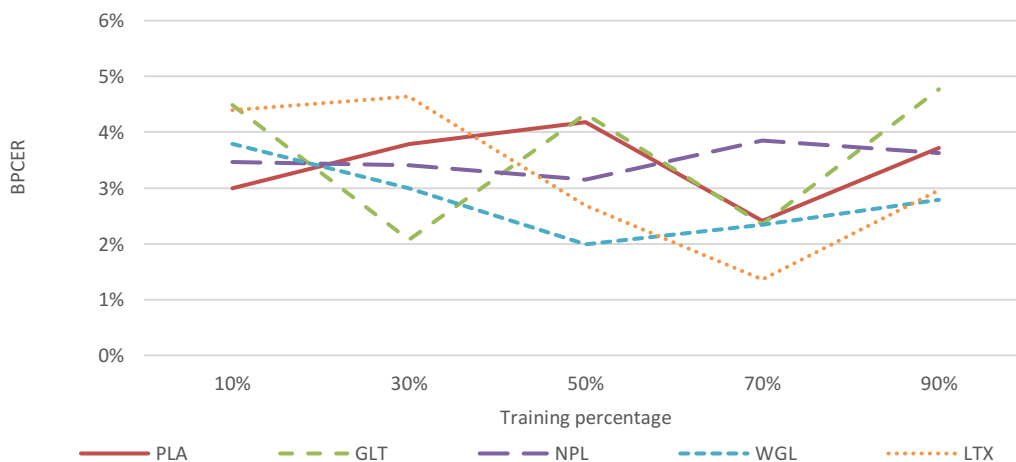
**Table 48. APCER and BPCER cross-comparison of 575/610nm wavelength samples in the red channel.**

	Training percentage				
	10%	30%	50%	70%	90%
APCER	9.36	4.07	3.99	1.78	0.89
BPCER	7.04	2.92	1.11	1.33	2.79

According to ISO/IEC 30107-3, APCER and BPCER shall be calculated separately by PAI species. Thus, this subsection gathers the different results achieved per fake finger material, using the 575/610nm lighting mode and taking the red channel. The cross-comparisons for APCER and BPCER can be seen on Figure 62 and Figure 63.



**Figure 62. APCER cross-comparison with different PAI species. PLA = Play-Doh, GLT = gelatin, NPL = nail polish, WGL = white glue, LTX = latex.**



**Figure 63. BPCER cross-comparison with different PAI species. PLA = Play-Doh, GLT = gelatin, NPL = nail polish, WGL = white glue, LTX = latex.**

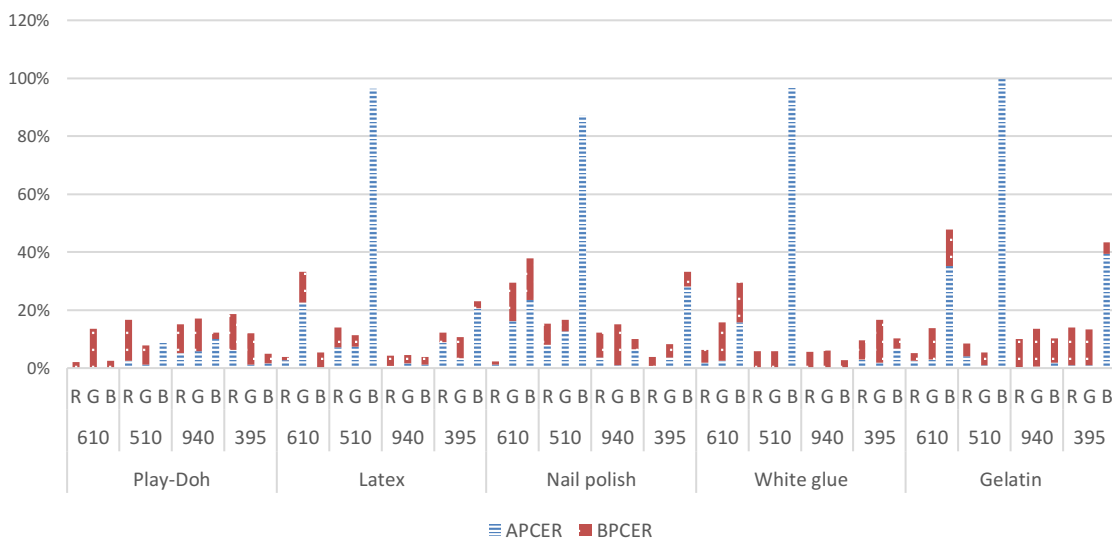
According to the graphs, the lowest APCER is clearly for the Play-Doh case (0%), followed by gelatin (1.64% at 70% training). For BPCER, latex gives the lowest error rate, 1.36% at 70% training, and Play-Doh, gelatin and white glue follow it with very similar rates: 2.41%, 2.35% and 2.34%, respectively.

8.2.3.3 By PAI species, wavelength and RGB channel

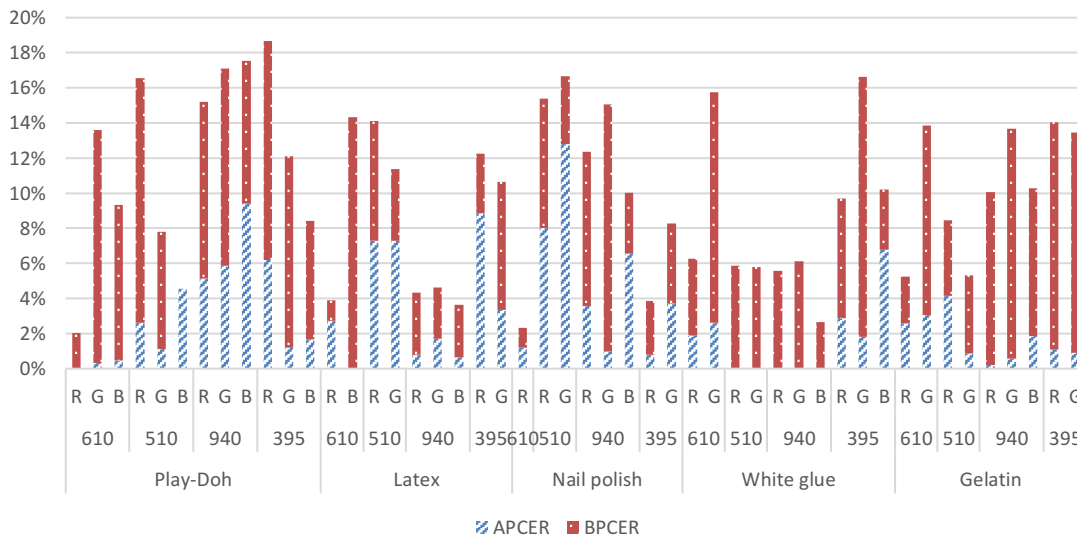
With the goal of having a more thorough study on wavelength and channel influence on the different materials, errors were calculated for each category classification. Channels R, G and B and wavelengths 575/610nm, 480/510nm, 940nm and 395nm were separated to calculate the different APCER and BPCER depending on the material put to the test. Results can be seen on Figure 64. For visualization purposes, the APCER + BPCER values greater than 20% are deleted on Figure 65. As it can be observed, some wavelengths and channels yield better error rates than others for different materials. For instance, the blue channel is the most problematic one when detecting fake fingers, with error rates as high as 96.54% for white glue in the 475/510nm wavelength. On the other hand, some channels and wavelengths produce very promising error rates. The lowest ones for each material are shown on Table 49 (70% of the samples were used for training). An interesting outcome is that, Play-Doh being the easiest to build PAI, it obtains also the lowest error rate.

**Table 49. Lowest error rates for each PAI species. Lower error rate considers the lowest APCER and BPCER combination.**

	<b>PLA</b>	<b>LTX</b>	<b>NPL</b>	<b>WGL</b>	<b>GLT</b>
<b>Difficulty to build PAI</b>	Easy	Easy	Easy	Easy	Medium
<b>APCER (%)</b>	0.00	1.20	1.19	0.00	2.59
<b>BPCER (%)</b>	2.03	2.67	1.12	2.67	2.67
<b>Wavelength</b>	610	940	610	940	610
<b>Color channel</b>	R	B	R	B	R



**Figure 64. APCER and BPCER calculated by PAI species, wavelength and RGB channel.**

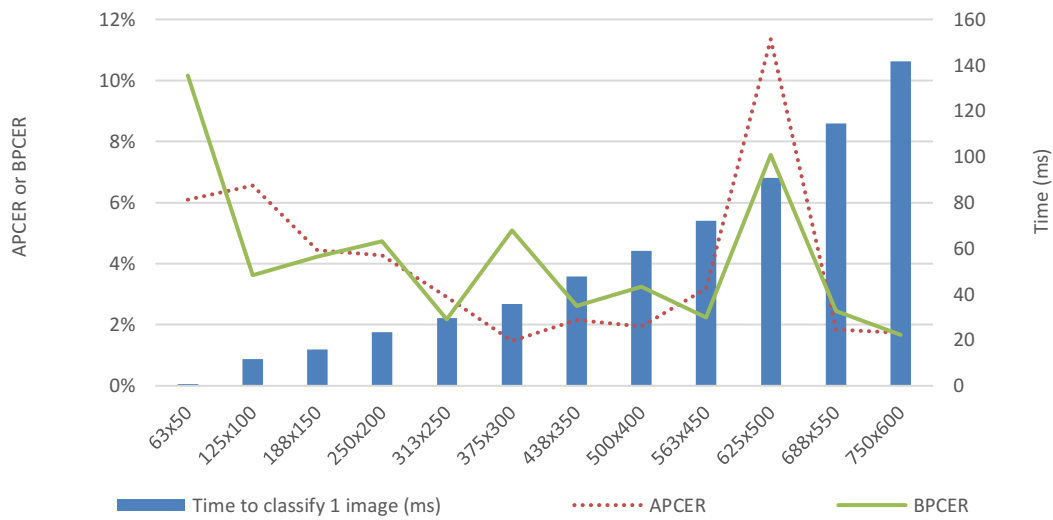


**Figure 65. APCER and BPCER calculated by PAI species, wavelength and RGB channel. APCER + BPCER outliers greater than 20% are deleted for clarification.**

### 8.2.3.4 Time performance vs. image size

The duration of a PAD subsystem classification is important for time-bound situations. A system that is meant for access control requires that the process for verification is fast, for convenience purposes. For other cases, like critical infrastructures where a high security level is required, taking more time might be acceptable in exchange for lower error rates.

To study this matter, images from the 575/610nm wavelength in the red channel were cropped to different sizes, from 50px to 600px, and then the algorithm was used again to check if the performance held at smaller sizes. Then, the time performance was calculated for each case, for classifying one image as real or fake. The PC used for the calculations is an Intel Core x64 i7-6700 CPU at 3.40GHz with 16GB RAM, using MATLAB. The results can be seen on Figure 66.



**Figure 66. APCER and BPCER results for different image sizes, as well as time elapsed for classifying 1 image.**

The graph shows an overview of the different trade-offs between size, error rates and time performance. For instance, at the 313x250px size, the error rates are quite low (2.91% APCER and 2.17% BPCER) while the time to classify one sample as real or fake is also low, 59.8ms, which could be a balanced trade-off. Both APCER and BPCER are best performing at the initial size, 750x600px (duration being 141.7ms); nevertheless, the size of 438x350 leads also to a low error rate, with an increase of 0.41% for APCER and 0,95% for BPCER (duration being 47.7ms).

### 8.2.3.5 Leaving out non-conformant fingerprints

As there is a user in the database with non-conformant fingerprints due to a skin disease, another classification was done leaving these samples out (90 fake and 36 real). As it can be seen on Table 50, APCER and BPCER are still similar to the values obtained including the user, meaning that the system can work even with non-conformant fingerprints, as it is represented on Table 51.

**Table 50. APCER and BPCER cross-comparison of 575/610nm wavelength samples in the red channel, leaving out one capture subject’s non-conformant fingerprints due to a skin disease. Results were averaged 10 times.**

	Training percentage				
	10%	30%	50%	70%	90%
<b>APCER</b>	9.05	6.90	3.51	1.70	2.46
<b>BPCER</b>	3.25	2.02	1.49	1.17	1.25

**Table 51. Decrease of APCER and BPCER leaving out the capture subject with a skin disease.**

	Training percentage				
	10%	30%	50%	70%	90%
<b>Δ APCER</b>	-0,31	2,83	-0,48	-0,08	1,57
<b>Δ BPCER</b>	-3,79	-0,90	0,38	-0,16	-1,54

### 8.2.4 Conclusions

This chapter gathers a thorough evaluation on a presentation attack detection technique and proposes a novel method to acquire fingerprints, having carried out the capture (including selection of hardware and the design of capture tools) and processing, classification and results analysis. As an outcome, a low-cost and good performing PAD subsystem was obtained. This is meaningful because hardware solutions have barely been researched and there are scarce reports, and usually these methods yield a high cost.

First, a proof of concept experiment was carried out by using a narrow-band camera with a 10nm tunable filter. This made it possible to observe and classify fingerprints in different wavelengths. Then, 2 handheld microscopes with special lighting were used to perform a more thorough PAD evaluation, acquiring more fingerprints from more capture subjects and with a wider range of PAI species. In doing so, it was seen that it is possible to achieve a low APCER and BPCER values using only one wavelength (575nm) with a filter (610nm) and taking only the red channel, which makes it inexpensive and accurate (APCER of 1.78% and BPCER of 1.33% at 70% training). Moreover, although it must be more thoroughly tested and with a bigger database, all iterations of classifying the 480/510nm wavelength of the blue channel have shown a BPCER of 0,00%. Furthermore, it was discovered that Play-Doh artefacts are very easy to detect with this approach, which is a very commonly used material.

In addition, the database included one subject whose fingerprints did not have any noticeable ridges and valleys due to a skin disease, and it was seen that the attack detection error only improved very slightly when removing these samples. That means that this approach is also appropriate for these cases.

### 8.2.5 Contributions and dissemination

This work was part of the work done in collaboration with the Nara Institute of Science and Technology in Japan, in an 8-month mobility program. It resulted in a published journal paper.

#### 8.2.5.1 Journal paper

[107] I. Goicoechea-Telleria, K. Kiyokawa, J. L. Jimenez, and R. Sanchez-Reillo, "Low-cost and efficient hardware solution for presentation attack detection in fingerprint biometrics using special lighting microscopes," *IEEE Access*, vol. 7, pp. 1–1, 2019.

- PAD evaluation with special lighting microscopes.

#### 8.2.5.2 Standardization

No contribution could be done to the standards dealing with presentation attack detection, as it is already finished, and no further comments can be made. Nevertheless, contributions will be made when the revision is due.





# Chapter 9. Conclusions and future work

---

THIS CHAPTER DESCRIBES the general lessons that were learnt during the process of this work and gives suggestions for future work, as specific conclusions were previously detailed for each experiment and chapter.

## 9.1 Conclusions

Security evaluations are necessary to assess a device's ability to reject access to non-authorized users. To be able to make such evaluations, it is necessary to have a common ground so that they can be compared among researchers and certification bodies. Studies are only comparable if the same metrics and procedures are used. For this Thesis, a methodology was developed by joining the standards ISO/IEC 30107 [2], [92] and ISO/IEC 19989 [108], Common Criteria [18], a methodology for the evaluation of mobile devices [21] and a methodology for security evaluations [19], and it was applied to several PAD evaluations on different mobile devices with embedded fingerprint sensors and off-the-shelf desktop fingerprint readers [22], [23], [95], [97]–[99].

Along all studies, it was repeatedly proven that people with no expertise in attacking fingerprint devices could successfully attack them within a week or less, just by watching a video of a researcher doing it. Very similar videos are available on well-known online platforms for everyone to see. Moreover, the materials used were readily available in supermarkets on online marketplaces.

Another notable outcome is that the real difficulty of making fingerprints out of a latent print was put to the test, by finding an easier process to steal them and performing a PAD evaluation [97]. For that, a cell phone camera with the flash activated was used then processed automatically with a smartphone document scanner app. It was possible to reproduce fingerprints left behind on the screen by the genuine user and use them on the scanners of 5 smartphones. All smartphones were, again, successfully attacked.

Attack potential is an adequate tool to measure the effort needed to attack a system. Nevertheless, in the case of Biometrics it is difficult to calculate. Even within the same evaluation, the evaluator gets better at attacking the system in each attempt. Also, at any point of the process, anyone can get the trick to hacking a specific sensor (out of expertise and, mostly, out of luck) and the evaluation results can vary highly from that point on. To soften this variability, one solution is reporting examples of the molds, artefacts and captured images of the evaluation.

Once commercial desktop and mobile device readers were evaluated following ISO/IEC 30107, it was clearly seen that PAD mechanisms are urgently needed in the implementation of biometric systems. Thus, it was decided to develop a new technique for detecting presentation attacks. This part of the work gathers a thorough evaluation on a presentation attack detection technique and proposes a novel method to acquire fingerprints, having carried out the capture (including selection of hardware and the design of capture tools) and processing, classification and results analysis. As an outcome, a low-cost and good performing PAD subsystem was obtained [107]. This is meaningful because hardware solutions have barely been researched and there are scarce reports, and usually these methods yield a high cost.

It was seen that it is possible to achieve a low APCER and BPCER values using only one wavelength (575nm) with a filter (610nm) and taking only the red channel, which makes it inexpensive and accurate (APCER of 1.78% and BPCER of 1.33% at 70% training). Moreover, although it must be more thoroughly tested and with a bigger database, all iterations of classifying the 480/510nm wavelength of the blue channel have shown a BPCER of 0,00%. Furthermore, it was discovered that Play-Doh artefacts are very easy to detect with this approach, which is a very commonly used material.

In addition, the database included one subject whose fingerprints did not have any noticeable ridges and valleys due to a skin disease, and it was seen that the attack detection error only improved very slightly when removing these samples. That means that this approach is also appropriate for these cases.

Moreover, the security analysis of biometric mechanisms should include a risk analysis that meets the needs of the users and the final application. For instance, levels of comfort and security are different for a normal mobile phone usage and for a high security device. That is, even though currently biometric technologies are vulnerable, they do increase the level of security, needing more effort from the attacker to gain restricted information. With the inclusion of better presentation attack detection mechanisms, vulnerabilities could be highly reduced maintaining a good level of comfort. Therefore, Biometrics is a viable and powerful tool for identification systems.

In summary, the milestones achieved by this Thesis include:

- Improvements on the presentation attack detection evaluation methodology.
- Contributions to ISO/IEC 30107 - Biometric presentation attack detection - Part 3: *Testing and reporting* and Part 4: *Profile for evaluation of mobile devices*.
- Presentation attack detection evaluations on commercial desktop and smartphone fingerprint sensors following ISO/IEC 30107-3 and 4, considering different variables to study: cooperative vs. non-cooperative, time limitations, expertise.
- A new low-cost and efficient optical presentation attack detection system and an evaluation on the said system.

## 9.2 Future work

There are numerous lines of work than can stem from this Thesis, both on the PAD evaluation and PAD mechanism developing sides:

- **PAD evaluation:** in the future and in general, PAD evaluations should be performed with more than one attacker, as it was proven in this work that the IAPMR depends on the person performing the attacks. Also, more types of materials can be used for testing PAD mechanisms of both smartphone and desktop readers. Moreover, it would be interesting to study the artefact creation under different environmental conditions, as results may vary, as seen on this work. Furthermore, the difference in IAPMR between fingers could be studied, as different fingers yield different results. Lastly, a quality assessment could be performed along with the PAD attempts to check if there is any relationship between quality and attack performance.
- **PAD mechanisms:** the most important future work would be to gather a bigger user database. Along those lines, more attackers should perform the same types of attacks on the system, because as it was seen during this work, different evaluators obtain different results when attacking systems. Moreover, on the classification side, a plethora of more approaches can be explored for image pre-processing, as the classification algorithm was fed raw images. Furthermore, fusion methods could be examined by combining several wavelengths.

As current ongoing work, all the considerations explained in this Thesis are being discussed and contributed in ISO/IEC 30107 Parts 3 and 4, as a follow up of the contributions made by the author in previous phases of the standard.



---

# References

---

- [1] ISO / IECJTC 1 / SC37, "Text of FDIS 30107-3, Information technology – Biometric presentation attack detection – Part 3: Testing and reporting," *ISO-IEC Standards*, vol. 2008. 2009.
- [2] SC 37, "ISO/IEC 2nd WD 30107-4 Biometric presentation attack detection - Part 4: Profile for evaluation of mobile devices," 2018.
- [3] Common Criteria, "Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model September 2012 Revision 4," *Int. Organ. Stand. Int. Electrotech. Comm. ISO/IEC 15408 Common Criteria, Part 12012*, no. September, p. 93, 2012.
- [4] R. Blanco-Gonzalo, R. Sanchez-Reillo, J. Liu-Jimenez, and C. Sanchez-Redondo, "How to assess user interaction effects in Biometric performance," 2017.
- [5] D. He and D. Wang, "Robust Biometrics-Based Authentication Scheme for Multiserver Environment," *IEEE Syst. J.*, vol. 9, no. 3, pp. 816–823, 2015.
- [6] L. O’Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proc. IEEE*, vol. 91, no. 12, pp. 2021–2040, 2003.
- [7] T. van der Putte and J. Keuning, "Biometrical fingerprint recognition: don’t get your fingers burned," *Smart card Res. Adv. Appl. IFIP TC8/WG8. 8 Fourth Work. Conf. Smart Card Res. Adv. Appl. Sept. 20-22, 2000, Bristol, United Kingdom*, vol. 31, no. 0, p. 16, 2000.
- [8] S. Schuckers, "Spoofing and Anti-Spoofing Measures," *Inf. Secur. Tech. Rep.*, vol. 7, no. 4, pp. 56–62, 2002.
- [9] A. Choiniere and T. Lubysheva, *Novetta - Protecting against Fingerprint Vulnerabilities when Deploying Biometric Systems*. 2015.
- [10] J. Blommé, "Evaluation of biometric security systems against artificial fingers," 2003.
- [11] L. Ghiani, D. A. Yambay, V. Mura, G. L. Marcialis, F. Roli, and S. Schuckers, "Review of the Fingerprint Liveness Detection (LivDet) competition series: 2009 to 2015," *Image Vis. Comput.*, 2015.
- [12] Anders Wiehe, Torkjel Søndrol, Ole Kasper Olsen, and Fredrik Skarderud, "Attacking fingerprint sensors," 2004.
- [13] T. Matsumoto, S. Hoshino, H. Matsumoto, and K. Yamada, "Impact of Artificial ‘Gummy’ Fingers on Fingerprint Systems," 2002.
- [14] J. Galbally, J. Fierrez, J. Rodriguez-Gonzalez, F. Alonso-Fernández, J. Ortega-Garcia, and M. Tapiador, "On the Vulnerability of Fingerprint Verification Systems to Fake Fingerprints Attacks," 2006.
- [15] S. Schuckers, "Presentations and attacks, and spoofs, oh my," *Image Vis. Comput.*, 2016.
- [16] Frank, "Chaos Computer Club breaks Apple TouchID," 2013. [Online]. Available: <https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid>.
- [17] Alex Hern, "Hacker fakes German minister’s fingerprints using photos of her hands," *The Guardian*, 30-Dec-2014.
- [18] Common Criteria, "Common Methodology for Information Technology Security Evaluation Evaluation methodology September 2012 Revision 4 Foreword," *Ccmb-2012-09-004*, no. September, p. 433, 2012.
- [19] B. Fernandez-Saavedra, R. Sanchez-Reillo, and J. Liu-Jimenez, "Best Practices for the Security Evaluation of Biometric Systems," 2014.
- [20] B. Fernandez-Saavedra, R. Sanchez-Reillo, R. Alonso-Moreno, and C. Sanchez-Avila, "Evaluation methodology for fake samples detection in biometrics," *Proc. - Int. Carnahan Conf. Secur. Technol.*, pp. 233–240, 2008.
- [21] B. Fernandez-Saavedra and R. Sanchez-reillo, "Testing of Biometric Systems integrated in Mobile Devices," *IEEE Int. Carnahan Conf. Secur. Technol.*, p. 321–326, 2015.
- [22] I. Goicoechea-Telleria, J. Liu-Jimenez, R. Sanchez-Reillo, and W. Ponce-Hernandez, "Vulnerabilities of Biometric Systems integrated in Mobile Devices : an evaluation," *Int. Carnahan Conf. Secur. Technol.*, 2016.
- [23] I. Goicoechea-Telleria, B. Fernandez-Saavedra, and R. Sanchez-Reillo, "An Evaluation of Presentation Attack Detection of Fingerprint Biometric Systems applying ISO / IEC 30107-3," in *International Biometric Performance Testing Conference*, 2016.
- [24] S. E. Schuster, "Fingerprinting method," *IBM Technical Disclosure Bulletin: 12-70p1852*, 1970.

- [25] Wikipedia, "Thomas Bewick."
- [26] Wikipedia, "Jan Evangelista Purkyně."
- [27] "History of fingerprints."
- [28] Wikipedia, "Sir William Herschel."
- [29] "William James Herschel and the discovery of fingerprinting."
- [30] Wikipedia, "Henry faulds."
- [31] Wikipedia, "Sir Edward Henry."
- [32] T. Dunstone and N. Yager, *Biometric System and Data Analysis - Design, Evaluation, and Data Mining*. 2009.
- [33] ISO/IEC SC37, "19795-1 Biometric performance testing and reporting — Part 1: Principles and framework." 2018.
- [34] S. Memon, M. Sepasian, and W. Balachandran, "Review of finger print sensing technologies," *IEEE INMIC 2008 12th IEEE Int. Multitopic Conf. - Conf. Proc.*, pp. 226–231, 2008.
- [35] D. Harris, "Fingerprint authentication," 2007. [Online]. Available: <http://electronicdesign.com/components/fingerprint-authentication>.
- [36] P. D. Wasserman and G. Researcher, "Solid-state fingerprint scanners - a survey of technologies," 2005.
- [37] L. Thalheim and J. Krissler, "Body check: biometric access protection," 2002.
- [38] U. Uludag, "Attacks on biometric systems: a case study in fingerprints," *Proc. SPIE*, vol. 5306, pp. 622–633, 2004.
- [39] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli, and S. Schuckers, "LivDet 2011 - Fingerprint liveness detection competition 2011," *Proc. - 2012 5th IAPR Int. Conf. Biometrics, ICB 2012*, pp. 208–215, 2012.
- [40] L. Thalheim, J. Krissler, and P.-M. Ziegler, "Body Check: Biometrics Defeated," 2002. [Online]. Available: <http://www.pcmag.com/article2/0,2817,13919,00.asp>.
- [41] G. L. Marcialis et al., *LivDet 2009- Fingerprint Liveness Detection Competition 2009*. 2009.
- [42] L. Ghiani et al., "Livdet 2013 fingerprint liveness detection competition 2013," *Biometrics (ICB), 2013 Int. Conf.*, pp. 1–6, 2013.
- [43] V. Mura, L. Ghiani, G. L. Marcialis, F. Roli, D. A. Yambay, and S. A. Schuckers, "LivDet 2015 fingerprint liveness detection competition 2015," *2015 IEEE 7th Int. Conf. Biometrics Theory, Appl. Syst.*, 2015.
- [44] K. Cao and A. K. Jain, "Hacking Mobile Phones Using 2D Printed Fingerprints," 2016.
- [45] M. Sandstrom, "Liveness Detection in Fingerprint Recognition Systems," *Linköping University*, 2004.
- [46] S. J. E. P. D, S. K. Modi, L. Maccarone, M. R. Young, C. Jin, and H. K. P. D, "Image Quality and Minutiae Count Comparison for Genuine and Artificial Fingerprints," pp. 30–36, 2007.
- [47] C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: a survey," *Iet Biometrics*, vol. 3, no. 4, pp. 219–233, 2014.
- [48] M. Espinoza and C. Champod, "Using the Number of Pores on Fingerprint Images to Detect Spoofing Attacks."
- [49] S. M. and W. B. N. Manivanan, "Automatic detection of active sweat pores of fingerprint using highpass and correlation filtering," *Electron. Lett.*, vol. 46, no. 18, pp. 1268–1269, 2010.
- [50] H. Choi, R. Kang, K. Choi, and J. Kim, "Aliveness detection of fingerprints using multiple static features," *Int. J. Biol. Med. Sci.*, vol. 2, no. 3, pp. 200–205, 2007.
- [51] B. Tan and S. Schuckers, "New approach for liveness detection in fingerprint scanners based on valley noise analysis," *J. Electron. Imaging*, vol. 17, no. 1, p. 011009, 2008.
- [52] C. Jin and L. Shengzhe, "Fingerprint Liveness Detection Based on Multiple Image Quality Features," no. Jin, C., Shengzhe, L. (2011). *Fingerprint Liveness Detection Based on Multiple Image Quality Features*. Retrieved from [http://atibook.ir/dl/en/Engineering/Computer Science/9783642179549\\_information\\_security\\_applications.pdf#page=296](http://atibook.ir/dl/en/Engineering/Computer Science/9783642179549_information_security_applications.pdf#page=296), 2011.
- [53] E. Marasco and C. Sansone, "An anti-spoofing technique using multiple textural features in fingerprint scanners," *BioMS 2010 - 2010 IEEE Work. Biometric Meas. Syst. Secur. Med. Appl. Proc.*, pp. 8–14, 2010.
- [54] B. Tan and S. Schuckers, "Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 2006, pp. 1–8, 2006.
- [55] B. Tan and S. Schuckers, "Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise," *Pattern Recognit.*, vol. 43, no. 8, pp. 2845–2857, 2010.
- [56] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake finger detection by skin distortion

- 
- analysis,” *IEEE Trans. Inf. Forensics Secur.*, vol. 1, no. 3, pp. 360–373, 2006.
- [57] Y. Zhang, J. Tian, X. Chen, X. Yang, and P. Shi, “Fake Finger Detection Based on Thin-Plate Spline Distortion Model,” *Adv. Biometrics*, vol. 4642, pp. 742–749, 2007.
- [58] R. Derakhshani, S. Schuckers, L. A. Hornak, and L. O’Gorman, “Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners,” *Pattern Recognit.*, vol. 36, no. 2, pp. 383–396, 2003.
- [59] Y. Wei-Yun, T. Hai-Linh, and T. Eam-Khwang, “Fake finger detection using an electrotactile display system,” 2008 10th Int. Conf. Control. Autom. Robot. Vision, ICARCV 2008, no. December, pp. 962–966, 2008.
- [60] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, “Fake Fingerprint Detection by Odor Analysis,” *Adv. Biometrics*, vol. 3832, pp. 265–272, 2006.
- [61] V. Reddy, A. Kumar, and R. S.M.K., “A New Method for Fingerprint Antispoofing using Pulse Oximetry,” 2007.
- [62] R. K. Rowe, K. A. Nixon, and S. P. Corcoran, “Multispectral fingerprint biometrics,” *Proc. from 6th Annu. IEEE Syst. Man Cybern. Inf. Assur. Work. SMC 2005*, vol. 2005, pp. 14–20, 2005.
- [63] D. Zhang, Z. Guo, and Y. Gong, *Multispectral Biometrics: Systems and Applications*. 2015.
- [64] N. Ratha and V. Govindaraju, “Multispectral Fingerprint Image Acquisition,” *Adv. Biometrics*, pp. 3–23, 2008.
- [65] C. Sousedik, R. Breithaupt, and C. Busch, “Volumetric Fingerprint Data Analysis using Optical Coherence Tomography,” *Int. Conf. Biometrics Spec. Interes. Gr. (BIOSIG)*, 2013, pp. 51–62, 2013.
- [66] E. Auksorius and A. C. Boccara, “Fingerprint imaging from the inside of a finger with full-field optical coherence tomography,” *Biomed. Opt. Express*, vol. 6, no. 11, p. 4465, 2015.
- [67] M.-R. Nasiri-Avanaki, “Anti-Spoof Reliable Biometry of Fingerprints Using En-Face Optical Coherence Tomography,” *Opt. Photonics J.*, vol. 01, no. 03, pp. 91–96, 2011.
- [68] L. Ghiani, P. Denti, and G. L. Marcialis, “Experimental results on fingerprint liveness detection,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7378 LNCS, pp. 210–218, 2012.
- [69] S. B. Nikam and S. Agarwal, “Fingerprint liveness detection using curvet energy and co-occurrence signatures,” in *Proceedings - Computer Graphics, Imaging and Visualisation, Modern Techniques and Applications, CGIV, 2008*, pp. 217–222.
- [70] S. B. Nikam and S. Agarwal, “Wavelet energy signature and GLCM features-based fingerprint anti-spoofing,” *Proc. 2008 Int. Conf. Wavelet Anal. Pattern Recognition, ICWAPR*, vol. 2, pp. 717–723, 2008.
- [71] S. B. Nikam and S. Agarwal, “Gabor Filter-Based Fingerprint Anti-spoofing,” pp. 1103–1114, 2008.
- [72] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, “A high performance fingerprint liveness detection method based on quality related features,” *Futur. Gener. Comput. Syst.*, vol. 28, no. 1, pp. 311–321, 2012.
- [73] L. F. A. Pereira et al., “A fingerprint spoof detection based on MLP and SVM,” *Proc. Int. Jt. Conf. Neural Networks*, pp. 10–15, 2012.
- [74] S. B. Nikam and S. Agarwal, “Ridgelet-based fake fingerprint detection,” *Neurocomputing*, vol. 72, no. 10–12, pp. 2491–2506, 2009.
- [75] S. B. Nikam and S. Agarwal, “Texture and wavelet-based spoof fingerprint detection for fingerprint biometric systems,” *Proc. - 1st Int. Conf. Emerg. Trends Eng. Technol. ICETET 2008*, pp. 675–680, 2008.
- [76] E. Marasco and C. Sansone, “Combining perspiration- and morphology-based static features for fingerprint liveness detection,” *Pattern Recognit. Lett.*, vol. 33, no. 9, pp. 1148–1156, 2012.
- [77] B. DeCann, B. Tan, and S. Schuckers, “A novel region based liveness detection approach for fingerprint scanners,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5558 LNCS, pp. 627–636, 2009.
- [78] S. Nikam, S.B., Agarwal, “Wavelet-based multiresolution analysis of ridges for fingerprint liveness detection,” *Int. J. Inf. Comput. Sec.*, 2009.
- [79] J. Jia and L. Cai, “Fake finger detection based on time-series fingerprint image analysis,” *Adv. Intell. Comput. Theor. Appl. With Asp. Theor. Methodol. Issues*, pp. 1140–1150, 2007.
- [80] J. Jia, L. Cai, K. Zhang, and D. Chen, “A new approach to fake finger detection based on skin elasticity analysis,” *Adv. Biometrics*, pp. 309–318, 2007.
- [81] Y. Cheng and K. V. Larin, “Artificial fingerprint recognition by using optical coherence tomography with autocorrelation analysis,” *Appl. Opt.*, vol. 45, no. 36, p. 9238, 2006.

- [82] Y. C. Y. Cheng and K. V. Larin, "In Vivo Two- and Three-Dimensional Imaging of Artificial and Real Fingerprints With Optical Coherence Tomography," *IEEE Photonics Technol. Lett.*, vol. 19, no. 20, pp. 1634–1636, 2007.
- [83] C. Sousedik, R. Breithaupt, and C. Busch, "Volumetric Fingerprint Data Analysis using Optical Coherence Tomography," *Biometrics Spec. Interes. Gr. (BIOSIG), 2013 Int. Conf.*, pp. 1–6, 2013.
- [84] M. Menrath and R. Breithaupt, "Fingerprint with OCT," Fern-Universität Hagen in Cooperation with Bundesamt für Sicherheit in der Informationstechnik (BSI), 2011.
- [85] P. V. Reddy, A. Kumar, S. M. K. Rahman, and T. S. Mundra, "A new antispoofing approach for biometric devices," *IEEE Trans. Biomed. Circuits Syst.*, vol. 2, no. 4, pp. 328–337, 2008.
- [86] C. Hengfoss, A. Kulcke, G. Mull, C. Edler, K. Puschel, and E. Jopp, "Dynamic liveness and forgeries detection of the finger surface on the basis of spectroscopy in the 400-1650 nm region," *Forensic Sci. Int.*, vol. 212, no. 1–3, pp. 61–68, 2011.
- [87] S. Chang, K. V. Larin, Y. Mao, C. Flueraru, and W. Almuhtadi, "Fingerprint Spoof Detection Using Near Infrared Optical Analysis," *State art biometrics.*, vol. Chapter 3, no. May 2017, pp. 57–84, 2011.
- [88] C. Sousedik, R. Breithaupt, and C. Busch, "Volumetric Fingerprint Data Analysis using Optical Coherence Tomography."
- [89] IDEMIA, "Télécom SudParis and IDEMIA present BioDigital, a new biometric technology to combat identity spoofing," 2018. [Online]. Available: <https://www.idemia.com/press-release/telecom-sudparis-and-idemia-present-biodigital-new-biometric-technology-combat-identity-spoofing-2018-09-06>.
- [90] Thorlabs, "OCT Imaging Systems & Components." [Online]. Available: [https://www.thorlabs.com/navigation.cfm?guide\\_id=2039](https://www.thorlabs.com/navigation.cfm?guide_id=2039).
- [91] SC27, "ISO/IEC 19989 Committee Draft." International Standardization Organization, 2019.
- [92] ISO / IECJTC 1 / SC37, "CD 30107-3, Biometric presentation attack detection — Part 3: Testing and reporting," 2015.
- [93] ISO / IECJTC 1 / SC37, "DRAFT INTERNATIONAL STANDARD ISO / IEC DIS 30107-3 Information technology — Biometric presentation attack detection —," 2017.
- [94] NIST, "NIST Biometric Image Software," NIST Biometric Image Software, 2015. [Online]. Available: <http://www.nist.gov/itl/iad/ig/nbis.cfm>.
- [95] I. Goicoechea-Telleria, R. Sanchez-Reillo, J. Liu-Jimenez, and R. Blanco-Gonzalo, "Attack Potential Evaluation in Desktop and Smartphone Fingerprint Sensors: Can They Be Attacked by Anyone?," *Wirel. Commun. Mob. Comput. Hindawi*, vol. 2018, pp. 1–13, 2018.
- [96] I. Goicoechea-Telleria, "Vulnerabilities in Fingerprint Biometric Recognition," Master Thesis, Carlos III University of Madrid, 2015.
- [97] I. Goicoechea-Telleria, A. Garcia-peral, A. Husseis, and R. Sanchez-reillo, "Presentation Attack Detection Evaluation on Mobile Devices : Simplest Approach for Capturing and Lifting a Latent Fingerprint," in *International Carnahan Conference on Security Technology (ICCST)*, 2018.
- [98] I. Goicoechea-Telleria, J. Liu-Jimenez, H. Quiros-Sandoval, and R. Sanchez-Reillo, "Analysis of the attack potential in low cost spoofing of fingerprints," *Int. Carnahan Conf. Secur. Technol.*, vol. 2017–October, pp. 1–6, 2017.
- [99] R. B. Gonzalo, B. Corsetti, A. Husseis, and I. Goicoechea-Telleria, "Attacking a smartphone biometric fingerprint system : a novice's approach," *2018 Int. Carnahan Conf. Secur. Technol.*, vol. 675087, no. October, pp. 1–5, 2018.
- [100] Y. Tamura, T. Mashita, Y. Kuroda, K. Kiyokawa, and H. Takemura, "Feature detection in biological tissues using multi-band and narrow-band imaging," *Int. J. Comput. Assist. Radiol. Surg.*, vol. 11, no. 12, pp. 2173–2183, 2016.
- [101] C. Schmid, "Bag-of-features for category classification," *ENS/INRIA Vis. Recognit. Mach. Learn.*, 2011.
- [102] S. Lazebnik *et al.*, "a Sparse Texture Representation Using Affine-Invariant Neighborhoods Regions To cite this version : A Sparse Texture Representation Using Affine-Invariant Regions," 2010.
- [103] J. Zhang, M. Marszałek, S. Lazebnik, and C. Schmid, "Local features and kernels for classification of texture and object categories: A comprehensive study," *Int. J. Comput. Vis.*, vol. 73, no. 2, pp. 213–238, 2007.
- [104] K. Tanaka, Y. Mukaigawa, H. Kubo, Y. Matsushita, and Y. Yagi, "Recovering Inner Slices of Layered Translucent Objects by Multi-Frequency Illumination," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, no. 4, pp. 746–757, 2017.
- [105] A. Krishnaswamy and G. V. G. Baranoski, "A Study on Skin Optics," *Tech. Rep. CS200401*, pp.



- 
- 1–17, 2004.
- [106] I. V. Meglinski and S. J. Matcher, “Quantitative assessment of skin layers absorption and skin reflectance spectra simulation in the visible and near-infrared spectral regions,” *Physiol. Meas.*, vol. 23, no. 4, pp. 741–753, 2002.
- [107] I. Goicoechea-Telleria, K. Kiyokawa, J. L. Jimenez, and R. Sanchez-Reillo, “Low-cost and efficient hardware solution for presentation attack detection in fingerprint biometrics using special lighting microscopes,” *IEEE Access*, vol. 7, pp. 1–1, 2019.
- [108] “ISO/IEC JTC 1/SC 27/WG 3 - Information technology - Security techniques - Security evaluation, testing and specification,” 2016.