# Attacking a smartphone biometric fingerprint system: a novice's approach

R. Blanco Gonzalo, B. Corsetti, *I. Goicoechea-Telleria, A. Husseis, J. Liu-Jimenez, R. Sanchez-Reillo
*Universidad Carlos III de Madrid*
Madrid, Spain
*igoicoec@ing.uc3m.es

T. Eglitis, E. Ellavarason, *R. Guest, C. Lunerti
*University of Kent*
Canterbury, UK
*r.m.guest@kent.ac.uk

*M. Azimi, J. Khiarak
*Politechnika Warszawska*
Warsaw, Poland
*m.azimi@elka.pw.edu.pl

*S. Ezennaya-Gomez, N. Whiskerd
*Otto-von-Guericke-Universität*
Magdeburg, Germany
*salatiel.ezennaya@ovgu.de

*R. Kuzu, E. Okoh
*Università Roma Tre*
Rome, Italy
*ridvansalih.kuzu@uniroma3.it

***Abstract*— Biometric systems on mobile devices are an increasingly ubiquitous method for identity verification. The majority of contemporary devices have an embedded fingerprint sensor which may be used for a variety of transactions including unlock a device or sanction a payment. In this study we explore how easy it is to successfully attack a fingerprint system using a fake finger manufactured from commonly available materials. Importantly our attackers were novices to producing the fingers and were also constrained by time. Our study shows the relative ease that modern devices can be attacked and the material combinations that lead to these attacks.**

***Keywords— biometric systems, fingerprints, spoofing, attack assessments)***

## I. Introduction

The growth in the use of mobile devices for everyday communication and transactions requires usable and secure methods of verifying the identity of a user. Biometric systems (verification though a personal characteristic or trait) are widely deployed on modern mobile devices where both general sensors (such as a camera or microphone) or specific biometric sensors (for example a fingerprint capture device) enable the donation of samples. Aided by open operating system interaction, the use of biometrics as a verification method is finding new uses beyond the conversional device unlock or transactional verification.

Fingerprint is the most widely used biometric on mobile devices. This popularity potentially leads to high gains in attacking or spoofing ownership of the finger. Many studies have investigated methods for generating 'fake fingers' but these are usually lead by ethical hacking groups or researchers with a large expertise in biometric systems research. In this current study, we wished to explore how easy it is for relative novices, using materials readily available on-line or in local shops and using open internet searches for background research, to create a fake finger and successfully attack a range of contemporary mobile devices. Our motivation for this study is twofold. Firstly, we wish to ascertain the ease with which successful fingerprints can be generated. Secondly, by exploring the materials that lead to a successful attack, we illustrate new areas for preventative research for future sensors.

## II. Mobile Device Fingerprint Spoofing

A biometric system can be vulnerable at many points: at presentation level, identity claim, data transfer, quality and feature extraction, decision thresholds, etc. [1] and this also applies to biometric sensors embedded in mobile devices. For instance, vulnerabilities were found creating a malicious application that steals the temporary fingerprint image by accessing its memory space or extracting a stored template from the non-volatile memory and recreating the feature points of the fingerprint [2]. In addition, several security analyses have been made using altered fingerprints [3], [4] and one was performed specifically on mobile devices [5]. This paper will focus on presentation attacks, that is, a presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system [6].

Presentation attacks can be overcome in several ways, divided in two groups: software and hardware PAD (Presentation Attack Detection) mechanisms [7]. Software PAD mechanisms read the captured sample and perform image processing and classification to distinguish whether the finger is real or not. Hardware PAD adds additional sensors (temperature sensor, multispectral cameras, etc. [8]) to make this distinction. Hardware solutions have lower error rates than the software ones [9] but are in general more expensive or bulky due to the additional equipment needed [8]. Thus, hardware mechanisms are usually not considered for mobile devices, as these solutions should be as cheap and small as possible.

Many studies and evaluations have been carried out regarding presentation attacks on desktop fingerprint sensors. Already in 1990, several sensors were tested using artefacts, and the system failed to reject them even from the first attempt [10]. On 2000, an evaluation was performed on [11] by calculating the acceptance rate of 1 user's finger made with gelatine on 11 scanners, 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

This work was supported by the EU Horizon 2020 Framework for Research and Innovation under Grant Agreement Number 675087 (AMBER)

978-1-5386-7931-9/18/$31.00 ©2018 European Union

were successful using latent fingerprint reactivation on 6 capacitive, 2 optical and 1 thermal sensors [12]. In [13], 10 capture subjects' fingers were used to create gelatine artefacts and use them on 3 sensors, getting success rates from 44.6% to 76%. On all experiments, only index fingers were used. Nevertheless, in general, 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 Liveness Detection (LivDet) competitions started in 2009 [14] and continued on 2011 [15], 2013 [16] and 2015 [17]. Their goal was to compare different liveness detection (Presentation Attack Detection, as required by the standard ISO/IEC 30107-3 [6]) mechanisms by using them on a very large database of fake fingers (made of gelatine, 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.

There are a number of reports on vulnerabilities that were found in mobile devices. In 2013, when the first iPhone with an embedded fingerprint sensor came out, the Chaos Computer Club [18] proved that it was possible to fool the sensor 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 very basic image processing. Nonetheless, this was only reported once in a video, no evaluation was performed. In 2016, fake fingers were printed using conductive silver ink. The researchers had a processed sample of the fingerprint image beforehand, so they could be used directly on the mobile phone sensor without having the additional step of creating moulds [19]. This was a technical report to inform about the vulnerability.

In 2018, an article reported on 3 different PAD evaluations on desktop and mobile device fingerprint sensors [20]. First, 4 desktop fingerprint sensors of different technologies were evaluated by attacking them with 7 different fake finger materials. All of them were successfully attacked by an experienced attacker. Secondly, a similar test was carried out on 5 smartphones with embedded sensors using the most successful materials from the previous evaluation, which also hacked the 5 sensors. Lastly, 15 simulated attackers with no background in biometrics were gathered to create fake fingers of several materials, and they had one week to attack the fingerprint sensors of the same 5 smartphones, with the starting point of a short video with the techniques to create them. All 5 smartphones were successfully attacked by an inexperienced attacker.

## III. The Challenge

The 'novice' participants in our study were all Research Fellows from the EU AMBER project. Although each of the Fellows were in the first year of their studies in biometric systems research, none had undertaken work directly related to fingerprint spoofing. 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 a variety of Android-based smartphones. Whilst it is possible to hypothesise that a seasoned hacker would have access to materials, techniques and expertise to maximise their chances of success, we were interested in exploring the performance of techniques implemented by non-experts. The three key factors in undertaking this study were that:

1. Participants had no previous direct experience of fingerprint spoofing.
2. Materials used were able to be purchased through outlets such as Amazon or supermarkets. Teams were able to research methods and materials on-line for a one-week period prior to the study.
3. Teams were limited a 12-hour development and testing limit.

An overview of the technology of the devices within the study are detailed in Table I. Note that the sensors on devices D4 and D5 are located on the rear of the device. Each of our devices are distinct in terms of sensor position or donation method (touch/swipe). All devices ran the Android operating system and used the standard method for capturing and comparing fingerprints for unlocking the device.

TABLE I. Mobile Devices Tested

| Device ID | Screen Size | Fingerprint Sensor Shape | Fingerprint Sensor Location | Fingerprint Sensor Type |
|---|---|---|---|---|
| D1 | 5.1" | Rectangular | Front | Touch |
| D2 | 5.7" | Rectangular | Front | Swipe |
| D3 | 5.2" | Rectangular | Side | Touch |
| D4 | 5.8" | Rectangular | Rear | Touch |
| D5 | 5.2" | Circular | Rear | Touch |

There are two different methodologies for fabricating fake fingerprints:

- Direct casts: A target is asked to press her/his finger on a material which is soft and mouldable but hardens with time or when cooled or heated. Using this fabrication process, high quantity moulds can be produced, achieving a fully three-dimensional sample of original print.
- Indirect casts: In this methodology, there is no need for cooperation of the target. Indirect casts can be pulled from latent fingerprints retrieved from natural secretions left by friction ridge skin on a surface during a contact or from a high-quality image of the finger. In comparison with the direct method, this method requires more complicated fabrication techniques.

In the interests of time, all the teams used a direct cast method of creating the fake finger. These methods relied on the creation of a mould from which an artefact was created. Given the limited time constraints, the teams focused on exploratory efforts at the expense of scientific rigour. With the limited time it was not feasible to use materials and methods which required long or multiple periods to set/harden. The methods used can be separated into the processes of creating a mould and creating a Presentation Attack Instrument (PAI or artefact)

from the mould. In this section we detail the processes trialled in the production of these elements.

### A. Mould Materials

A series of materials were trialled wherein a finger was directly applied to a formed ball of a pliable material (denoted as 'dry moulds') including: BluTack™, Plasticine™, Siligum™, unbranded Silicon Gum and Play-Doh™. Other materials that were unsuccessful in forming dry moulds were: magic putty, rubber putty, chewing gum and clay.

Three other methods were used to create a 'hot mould'. In both these methods a finger was inserted into the heated/melted substance which was then allowed to cool to form the mould: hot glue, candle wax and stamp wax. An attempt was made to form a mould from melted gummy sweets, however this was unsuccessful.

Fig. 1a and 1b shows two formed dry moulds from two different materials, whilst Fig. 1c shows the donation process with a third material.

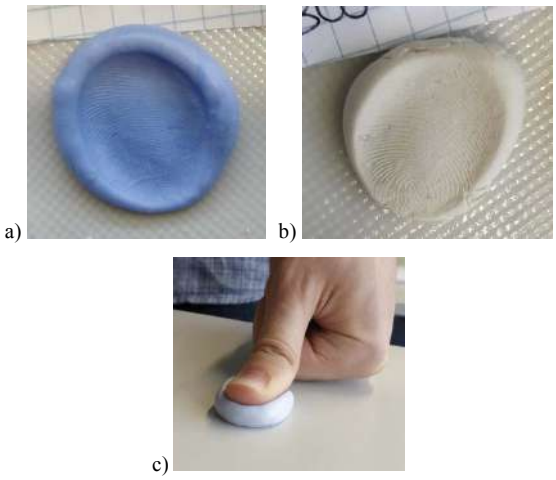

Fig. 1. a) Siligum mould, b) BluTack mould, c) mould creation process

### B. Presentation Attack Instrument (PAI)

The formation of PAIs can be divided into a 'dry' subcategory which were formed by pressing the material directly into a mould. 'Wet' materials were either substances that were heated, inserted into the mould and allowed to cool, or were in liquid form and subsequently dried in the mould. In all cases, the formed instrument was removed from the mould and directly presented to a mobile device fingerprint sensor.

The range of dry materials used were: Plasticine, Plasticine + conductive paint, Play-Doh and BluTack.

The wet materials trialled within the experiments were: art glue, art glue + graphite, alginate, gelatine powder, gelatine powder + glycerine, gelatine powder + conductive ink, gelatine sheet, gelatine + graphite, gelatine + water, candle wax, body wax + conductive paint and face mask. A further method, art glue, did not rely on the use of mould. Fig. 2 shows two gelatine-based PAI samples.

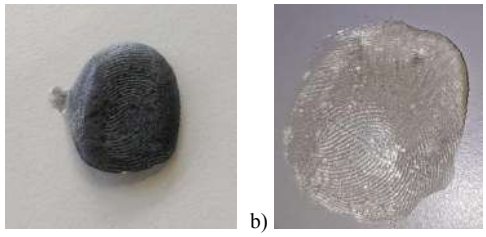

Fig. 2. A gelatine based PAI a) with and b) without added graphite.

A total of 35 experiments with different combinations of mould and PAI were conducted across three groups and the five devices. Table 2 shows the numeric identifier for each combination of materials. Given the timescale of the activity it was not possible to conduct a comprehensive evaluation of each combination, however each mould and PAI material was used at least once. The verification trial method followed the same protocol for all attempts:

1. A genuine finger is enrolled on a particular device following the standard in-build operating system enrolment protocol.
2. A PAI generated from the enrolled genuine finger is presented to the same device in an attempt to unlock/access the phone.
3. Whether the PAI was recognised as a 'finger', the number of presentations and the number of successful unlock/access were recorded.

## IV. Results

Table III shows the results from each of the individual experiments. A majority (25 out of 35) of PAIs were recognised as 'finger' by a device, indicating the relative ease within which a finger can be mimicked. The number of successful attack verifications were varied, with only one experiment achieving 100% attack success for each presentation (experiment 21). 16 out of the 35 PAIs resulted in at least one successful attack on the system, with 9 PAIs being recognised as a finger but not leading to a successful verification.

It is possible to explore the 35 PAI results in a number of ways. Table IV shows the number of successful attacks on each device. It is evident that there is considerable variation across sensors and systems. D4 was not compromised, however only two experiments were conducted on this device – in each case, the sensor could not detect a finger. Device D3 produced the poorest performance in terms of attack with 75% of presentation attempts being erroneously verified. There seems to be no significant performance difference between swipe and touch sensor technology.

Table V details the results separated by mould material. Siligum resulted in the highest number of successful attacks, nearly double the next successful material (candle wax). Siligum was used in the highest number of experiments, reflecting the experience of the novice researcher in that once they had discovered a successful mould material, this was used for subsequent experiments across various PAIs. A number of

moulds (BluTack, no mould and unbranded silicon) resulted in PAIs that unable to spoof the valid finger.

TABLE IV. ATTEMPTS AND SUCCESSFUL ATTACKS FOR EACH DEVICE

| Device | Number of Experiments | Number of Detections | Number of Presentations | Number of Successful Attacks | IAPMR |
|---|---|---|---|---|---|
| D1 | 15 | 8 | 115 | 23 | 20.0% |
| D2 | 4 | 4 | 50 | 3 | 6.0% |
| D3 | 4 | 4 | 52 | 39 | 75.0% |
| D4 | 2 | 0 | 0 | 0 | 0.0% |
| D5 | 10 | 9 | 142 | 25 | 17.6% |

TABLE V. ATTEMPTS AND SUCCESSFUL ATTACKS FOR EACH MOULD MATERIAL

| Mould | Number of Experiments | Number of Detections | Number of Presentations | Number of Successful Attacks | IAPMR |
|---|---|---|---|---|---|
| BluTack | 3 | 0 | 0 | 0 | 0.0% |
| Candle wax | 1 | 1 | 10 | 2 | 20.0% |
| Hot glue | 5 | 4 | 50 | 9 | 18.0% |
| No mould | 2 | 1 | 10 | 0 | 0.0% |
| Plasticine | 3 | 2 | 60 | 7 | 11.7% |
| Play-Doh | 1 | 0 | 0 | 0 | 0.0% |
| Siligum | 18 | 15 | 204 | 70 | 34.3% |
| Stamp wax | 1 | 1 | 13 | 2 | 15.4% |
| Unbranded silicon | 1 | 1 | 12 | 0 | 0.0% |

Table BI explores the material used to create the PAI. It can be observed that a number of materials with additives (art glue + graphite, body wax + conductive paint and gelatine sheet + graphite) perform well. Alginate as pure substance also produced a 51.7% success rate.

TABLE VI. ATTEMPTS AND SUCCESSFUL ATTACKS FOR EACH PAI MATERIAL

| PAI | Num of Experiments | Number of Detections | Number of Presentations | Number of Successful Attacks | IAPMR |
|---|---|---|---|---|---|
| Alginate | 3 | 3 | 60 | 31 | 51.7% |
| Art Glue | 3 | 1 | 10 | 0 | 0.0% |
| Art glue + graphite | 2 | 2 | 30 | 22 | 73.3% |
| BluTack | 1 | 0 | 0 | 0 | 0.0% |
| Body wax + conductive paint | 2 | 2 | 22 | 9 | 40.9% |
| Candle wax | 1 | 0 | 0 | 0 | 0.0% |
| Candle wax + conductive ink | 1 | 0 | 0 | 0 | 0.0% |
| Facemask | 1 | 0 | 0 | 0 | 0.0% |
| Gelatine powder | 3 | 2 | 23 | 0 | 0.0% |
| Gelatine powder + conductive ink | 1 | 1 | 11 | 0 | 0.0% |
| Gelatine powder + glycerine | 1 | 1 | 22 | 0 | 0.0% |
| Gelatine sheet | 7 | 4 | 69 | 9 | 13.0% |
| Gelatine sheet + graphite | 4 | 4 | 47 | 14 | 29.8% |
| Gelatine sheet + water | 2 | 2 | 30 | 3 | 10.0% |
| Plasticine | 1 | 1 | 10 | 1 | 10.0% |
| Plasticine + conductive paint | 1 | 1 | 10 | 1 | 10.0% |
| Play-Doh | 1 | 1 | 15 | 0 | 0.0% |

## V. CONCLUSIONS

In this work we have shown that it is possible, with limited experience and using available materials, to successfully attack a range of contemporary mobile devices using biometric fingerprints. In doing so we have demonstrated the material combinations that lead to successful (and unsuccessful) combinations. We recognise that this study is not without its limitations: i) each material was not tested on multiple fingers or across multiple users, ii) different versions of Android were installed across the devices, which may contain different fingerprint recognition algorithms/systems, iii) there was no sample quality assessment of the PAIs which would indicate the likely performance/consistency of the formed attack instrument. Despite the limitations, we have illustrated a range of techniques that can be explored further in terms of spoofing attack and future prevention.

## REFERENCES


[1] T. Dunstone and N. Yager, Biometric System and Data Analysis - Design, Evaluation, and Data Mining. 2009.

[2] Y. H. Jo, S. Y. Jeon, J. H. Im, and M. K. Lee, "Security analysis and improvement of fingerprint authentication for smartphones," Mob. Inf. Syst., vol. 2016, no. Krait 400, 2016.

[3] S. Yoon, J. Feng, and A. K. Jain, "Altered fingerprints: Analysis and detection," IEEE Trans. Pattern Anal. Mach. Intell., vol. 34, no. 3, pp. 451–464, 2012.

[4] A. K. Jain and S. Yoon, "Automatic detection of altered fingerprints," Computer (Long. Beach. Calif)., vol. 45, no. 1, pp. 79–82, 2012.

[5] S. Ghouzali, M. Lafkih, W. Abdul, M. Mikram, M. El Haziti, and D. Aboutajdine, "Trace Attack against Biometric Mobile Applications," Mob. Inf. Syst., vol. 2016, 2016.

[6] 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.

[7] S. C. Schuckers, "Spoofing and Anti-Spoofing Measures," Inf. Secur. Tech. Rep., vol. 7, no. 4, pp. 56–62, 2002.

[8] E. Marasco and A. Ross, "A Survey on Anti-Spoofing Schemes for Fingerprint Recognition Systems," 2014.

[9] D. Zhang, Z. Guo, and Y. Gong, "Multispectral Biometrics: Systems and Applications," Multispectral Biometrics Syst. Appl., pp. 1–229, 2015.

[10] 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.

[11] T. Matsumoto, S. Hoshino, H. Matsumoto, and K. Yamada, "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems," 2002.

[12] 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.

[13] J. Blommé, "Evaluation of biometric security systems against artificial fingers," 2003.

[14] G. L. Marcialis et al., LivDet 2009- Fingerprint Liveness Detection Competition 2009. 2009.

[15] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli, and S. A.C. Schuckers, "LivDet 2011 - Fingerprint liveness detection competition 2011," Proc. - 2012 5th IAPR Int. Conf. Biometrics, ICB 2012, pp. 208–215, 2012.

[16] L. Ghiani et al., "Livdet 2013 fingerprint liveness detection competition 2013," Biometrics (ICB), 2013 Int. Conf., pp. 1–6, 2013.

[17] 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.

[18] Frank, "Chaos Computer Club breaks Apple TouchID," 2013. [Online]. Available: https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid.

[19] K. Cao and A. K. Jain, "Hacking Mobile Phones Using 2D Printed Fingerprints," 2016.

[20] 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.

TABLE II. DEVICES AND MATERIALS TESTED

| PAI | | Plasticine | Plasticine + conductive paint | Play-Doh | BluTack | Art glue | Art glue + graphite | Alginate | Gelatine powder | Gelatine powder + glycerine | Gelatine powder + conductive | Gelatine sheet | Gelatine sheet + graphite | Gelatine sheet + water | Candle wax | Candle wax + conductive ink | Body wax + conductive paint | Face Mask |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | *Dry* | | | | *Wet* | | | | | | | | | | | | |
| **Mould** | | | | | | | | | | | | | | | | | | |
| **BluTack** | ***Dry*** | | | | | 1 | | | 2 | | | 33 | | | | | | |
| **Plasticine** | | | | | | | | | | | | 25, 34 | | 26 | | | | |
| **Siligum** | | 1 6 | | 3 | 4 | | 17, 18 | 19, 20, 21 | 5 | 6 | 7 | 8 | 9, 10 | | 11 | 12 | 22, 23 | |
| **Unbranded silicon** | | | | | | | | | 13 | | | | | | | | | |
| **Play-Doh** | | | | | | 14 | | | | | | | | | | | | |
| **Hot glue** | ***Wet*** | | 32 | | | | | | | | | 27, 35 | 29 | 28 | | | | |
| **Candle wax** | | | | | | | | | | | | 30 | | | | | | |
| **Stamp wax** | | | | | | | | | | | | | 31 | | | | | |
| **No mould** | | | | | | | | | | | | | | | | | | 15 |

TABLE III. LIST OF EXPERIMENTS AND ATTACK RESULTS

| Experiment Number | Device | Group | Mould | PAI | Recognised | Presentations | Successes | IAPMR (Impostor Attack Presentation Match Rate) |
|---|---|---|---|---|---|---|---|---|
| 1 | D1 | 1 | BluTack | Art glue | ✗ | | | |
| 2 | D1 | 1 | BluTack | Gelatine powder | ✗ | | | |
| 3 | D1 | 1 | Siligum | Play-Doh | ✓ | 15 | 0 | 0.0% |
| 4 | D1 | 1 | Siligum | BluTack | ✗ | | | |
| 5 | D1 | 1 | Siligum | Gelatine powder | ✓ | 11 | 0 | 0.0% |
| 6 | D1 | 1 | Siligum | Gelatine powder + glycerine | ✓ | 22 | 0 | 0.0% |
| 7 | D1 | 1 | Siligum | Gelatine powder + conductive ink | ✓ | 11 | 0 | 0.0% |
| 8 | D1 | 1 | Siligum | Gelatine sheet | ✓ | 9 | 0 | 0.0% |
| 9 | D1 | 1 | Siligum | Gelatine sheet + graphite | ✓ | 5 | 2 | 40.0% |
| 10 | D5 | 1 | Siligum | Gelatine sheet + graphite | ✓ | 9 | 5 | 55.5% |
| 11 | D1 | 1 | Siligum | Candle wax | ✗ | | | |
| 12 | D1 | 1 | Siligum | Candle wax + conductive ink | ✗ | | | |
| 13 | D1 | 1 | Unbranded silicon | Gelatine powder | ✓ | 12 | 0 | 0.0% |
| 14 | D1 | 1 | Play-Doh | Art Glue | ✗ | | | |
| 15 | D1 | 1 | No mould | Facemask | ✗ | | | |
| 16 | D3 | 2 | Siligum | Plasticine | ✓ | 10 | 1 | 10.0% |
| 17 | D2 | 2 | Siligum | Art glue + graphite | ✓ | 10 | 3 | 30.0% |
| 18 | D3 | 2 | Siligum | Art glue + graphite | ✓ | 20 | 19 | 95.0% |
| 19 | D1 | 2 | Siligum | Alginate | ✓ | 30 | 21 | 70.0% |
| 20 | D2 | 2 | Siligum | Alginate | ✓ | 20 | 0 | 0.0% |
| 21 | D3 | 2 | Siligum | Alginate | ✓ | 10 | 10 | 100.0% |
| 22 | D2 | 2 | Siligum | Body wax + conductive paint | ✓ | 10 | 0 | 0.0% |
| 23 | D3 | 2 | Siligum | Body wax + conductive paint | ✓ | 12 | 9 | 75.0% |
| 24 | D2 | 2 | No mould | Art Glue | ✓ | 10 | 0 | 0.0% |
| 25 | D5 | 3 | Plasticine | Gelatine sheet | ✓ | 40 | 5 | 12.5% |
| 26 | D5 | 3 | Plasticine | Gelatine sheet + water | ✓ | 20 | 2 | 10.0% |
| 27 | D5 | 3 | Hot glue | Gelatine sheet | ✓ | 10 | 2 | 20.0% |
| 28 | D5 | 3 | Hot glue | Gelatine sheet + water | ✓ | 10 | 1 | 10.0% |
| 29 | D5 | 3 | Hot glue | Gelatine sheet + graphite | ✓ | 20 | 5 | 25.0% |
| 30 | D5 | 3 | Candle wax | Gelatine sheet | ✓ | 10 | 2 | 20.0% |
| 31 | D5 | 3 | Stamp wax | Gelatine sheet + graphite | ✓ | 13 | 2 | 15.4% |
| 32 | D5 | 3 | Hot glue | Plasticine + conductive paint | ✓ | 10 | 1 | 10.0% |
| 33 | D5 | 3 | BluTack | Gelatine sheet | ✗ | | | |
| 34 | D4 | 3 | Plasticine | Gelatine sheet | ✗ | | | |
| 35 | D4 | 3 | Hot glue | Gelatine sheet | ✗ | | | |