PD.TVZ.HR

POLYTECHNIC & DESIGN Vol. 9, No. 4, 2021.

Mrežna inačica: ISSN 2459-6302
Tiskana inačica: ISSN 1849-1995

DOI: 10.19279/TVZ.PD.2021-9-4-16

ANALYSIS OF THE SECURITY OF SMARTPHONE FINGERPRINT AUTHENTICATION

Domagoj Tuličić, Marinko Žagar

Tehničko veleučilište u Zagrebu /Informatičko računarski odjel, Zagreb, Republika Hrvatska

ABSTRACT

Mobile phones have become very complex devices through which we perform business functions and transactions and use them in various secure authentication schemes. Such usage leads to the storage of various confidential data on mobile phones, the security of which depends on the authentication mechanisms on the smartphone itself. In this paper, we present the results of the research of the security mechanism (function) that protects smartphones with fingerprint biometrics and the resistance of the sensors against the deception by false fingerprints.

Keywords: *Smartphone Fingerprint Authentication, Fake Fingerprint, Fingerprint Spoofing, Fingerprint Fabrication, Fingerprint Sensor Deception, Fooling Biometric Fingerprint Sensor*

1. INTRODUCTION

We are witnessing a technological evolution of human society in which mobile phones have changed the way of our daily habits, work habits and even the way of entertainment. Mobile phones are not just communication devices, they are much more and it is hard to imagine life without them.

On mobile phones, we store different types of information in digital form, such as personal information, sensitive information we use when conducting our business, or other information that can highlight our lifestyle habits. As the former Director of Engineering at Google, Ray Kurzweil, once said, "Mobile phones are misnamed, they should be called gateways to human knowledge." We could paraphrase his statement and claim that mobile phones are misnamed, they should be called entrance to everyone's life. Like any other important entrance, it must be protected from unauthorized access. The way mobile phones protect access to information, features and to the functions of the mobile phone is called authentication. Andress [1] explained authentication generally as the set of methods we use to establish an identity assertion as true. In this generalized definition of authentication, the pronoun "we" refers to humans. Unlike humans, machines also have authentication methods that are quite different from those that refer to humans [2].

We have identified four different human authentication mechanisms or methods for mobile phones, such as PINs or passwords, unlock patterns, facial recognition, and fingerprint. As a result, the authentication mechanisms or methods can be divided into two main groups: biometric authentication and non-biometric authentication. In this paper, we will describe biometric authentication and the results of our research in which we tried to fool biometric fingerprint sensors placed in mobile phones and gain access to information and functions of mobile phones.

This research leans on previous conducted research [23] in which the main goal was knowing fingerprint biometrics, and its methods that are used for authorization and authentication and also well know methods for spoofing fingerprints. Here we go further and we developed another way of making false fingerprints that are much more consistent to the real fingerprint. The quality of this false fingerprint was tested on sensor of mobile phones for which their producers are claiming that they could not be fooled.

2. FINGERPRINT BIOMETRIC AUTHENTICATION IN MOBILE PHONES

Extensive insights into the morphogenesis of the fingerprint give us a very good explanation why this part of the human body is relevant for authentication mechanisms (methods) [3]. The ridges of each human finger, located on the underside of the fingertips, are the patterns left by humans when they touch the surface. These ridges are categorized into three main types or shapes which can be seen in the fingerprint image as loops, swirls and arches. Each of these shapes has details and variations of the shape and therefore they are unique to each person.

The dissimilarity and uniqueness of human fingerprints has been recognized throughout human history. In the early twentieth century, fingerprint recognition was officially recognized as a valid method of personal identification and became a standard routine in forensic science. Fingerprint identification agencies were established worldwide and criminal fingerprint databases were built [4].

The fact that fingerprints were used in forensics and served as the main method of identification led to the development of biometric systems or more specifically automated fingerprint identification systems (AFIS) [5]. This is supported by Malton, Maio, Jain and Prabhakar [4]. They claim that automated fingerprint recognition technology has now grown rapidly beyond forensic applications into civil and commercial applications. In fact, fingerprint-based biometric systems are so popular that they have become almost synonymous with biometric systems.

Anil et. all [6] also claim that the popularity of fingerprint recognition, especially in non-forensic applications, is due to the availability of sophisticated, practical, and low-cost sensors that can quickly capture a person's fingerprint with minimal or no intervention by a human operator. These compact fingerprint capture sensors have also been incorporated into many consumer devices such as laptops and mobile phones for authentication (verification) after it was proven that this technology and methods were successfully used for identification by law enforcement around the world.

In the case of mobile phones, the first biometric sensor was placed on the back of the Siemens mobile phone prototype in 1998 [5][7]. The first commercial mobile phone with fingerprint sensor that overcame the problems of the Siemens prototype was the Sagem MC 959 launched in 2000 [5]. After Sagem, other manufacturers started to launch mobile phones with biometric sensor, such as Fujitsu with the F505i model in February 2003 [7] or Pantech with the Pantech GI100 model in 2004 [8]. Ten years after the Fujitsu model, Apple launched the iPhone 5 and created a revolution in the use of fingerprint sensors in the mobile phone industry. This Apple phone used fingerprint sensor technology to securely unlock the phone. After that, all manufacturers started to follow Apple's example. First, their mobile phones had a so-called home button, a capacitive sensor placed on the phone to facilitate unlocking, and then they started using optical and ultrasonic sensors with the development of touchscreens for mobile phones.

Nowadays, biometric fingerprint authentication is not only used for security access to mobile phones, but it is also an important technology for authentication when making payments over the Internet.

These are the areas of mobile banking where biometric fingerprint sensors are used extensively. In Croatia, every user of mobile banking services of major Croatian banks has the option to choose fingerprint authentication to perform a transaction. Taking into account the above facts, fingerprint authentication with smartphones will play a major role in overall security.

3. FINGERPRINT SENSOR TECHNOLOGIES IN MOBILE PHONES

Nowadays, almost every mobile phone has a fingerprint sensor. Most of these sensors are hidden under the phone's touchscreen, or rather, the phones have an in-screen fingerprint scanner.

Since Synaptics Incorporated [9] announced in 2016 the first optically based fingerprint sensor for smartphones that can be hidden under the screen of the mobile phone, more and more mobile phone manufacturers are abandoning fingerprint scanners that are visibly placed on the phone in the form of the so-called home button (key) and are using newer techniques and technologies

The technologies used for the process of capturing the fingerprint are based on one of the four main techniques: capacitive, optical, thermal and ultrasonic [10]. In mobile phones, in our experience, we found only capacitive, optical and ultrasonic technologies while we did not find the thermal sensor in any of the mobile phones existing on the Croatian market. Moreover, in our search for mobile phones with thermal sensor, we found many sources mentioning this technique. But the descriptions of this technique refer exactly to an article titled "Transparent and flexible fingerprint sensor array with multiplexed detection of tactile pressure and skin temperature", which describes the development of the thermal sensor [11].

So, after this finding, we are left with capacitive, optical and ultrasonic sensors. In general, capacitive sensors or capacitive sensors are well described and explained technology due to their long presence in the field of sensors [12]. Optical and ultrasonic technologies used for mobile phone scanners are more recent, so the description and explanation of their operation can generally be found on manufacturers' websites or on various biometrics-related websites [13] [14]. Optical technology can be easily fooled with the fake fingerprint (even with the image of the fingerprint), this is not the case with ultrasonic technology.

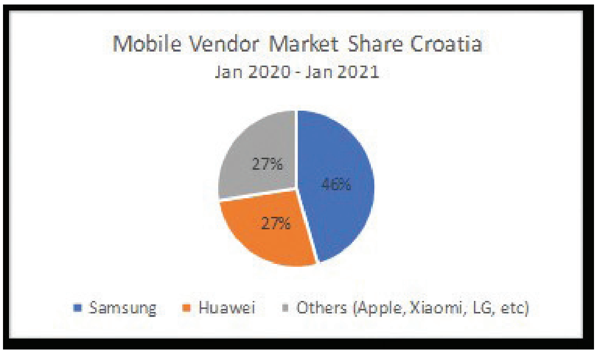

Figure 1 Mobile Vendor Market Share Croatia

Searching the websites of Qulacomm, the ultrasonic sensor manufacturer, for explanations of their product, we found that they make a fingerprint reader called 3D Sonic that uses technological advances and acoustics (sound waves) to scan the pores of a user's finger and create a very accurate 3D image. The manufacturer also claims that 3D Sonic uses acoustic-based technology that reflects the unique characteristics of a user's individual fingerprint, as opposed to optical solutions that expose the user to spoofing. With the built-in anti-spoofing, neither a photo nor a fake print of a finger can access your phone. Accordingly, the 3D Sonic sensor could be found in many flagship smartphones, including the Samsung Galaxy S10, Note10, S20, and Note20 series [15].

Considering the technologies mentioned earlier in our research, the following mobile phones with associated sensors were selected and presented in Table 1.

***Table 1.** Mobile phones types and sensor technologies*

MANUFACTURER	MODEL	SENSOR TECHNOLOGY
Samsung	S8	capacitive
Samsung	S10+	ultrasound
Samsung	S20	ultrasound
Huawei	P10 lite	capacitive
Huawei	P30 Pro	optical

With these mobile phones presented in Table 1. we have covered most of the mobile phone manufacturers on the Croatian market. More precisely, it is shown in the Figure 1. [16]. Considering that nowadays almost every phone has a fingerprint sensor, we can clearly see the prevalence of sensors in mobile phones.

4. CURRENT STATE OF METHODS FOR FINGERPRINT SPOOFING

According to Encyclopedia of Biometrics [17], there are three different methods and detection levels for fingerprint spoofing. In this section, we present these classifications starting from the easiest to the most difficult recognition.

These are:

1. Latent print left on the sensor

2. Fake/copies:

    a) Printed fingerprint image

    b) Fake made of gelatin, latex, or other material

    c) Thin layer of material glued to a real fingerprint, including real skin cell grown in a laboratory

3. Original fingerprint

    a) Cutout

    b) Belonging to a dead person

    c) Alive person under threat

Considering the second stage of the previous classification, we started searching for spoofing techniques or fingerprint forgery techniques by searching the World Wide Web. We chose the Google search engine because we believe that Google's results reflect the state of the community of enthusiasts interested in this field.

We used the phrases "fingerprint spoofing" and "fake fingerprint". A search for the first phrase "fingerprint spoofing" on Google showed over 8230 results in 0.40 seconds, [18] and a search for the second phrase "fake fingerprint" on Google showed over 31600 results in 0.44 seconds [19]. Then, for the phrase "fake fingerprint", we checked the 163 most relevant results according to the Google search engine. For the same phrase, we found over 2000 video contents, some of which are tutorials showing how to make a fake fingerprint. Using the same Google search results, we also looked at image results to try to identify methods or materials used to create a fake fingerprint.

We repeated the same procedure for the phrase "fingerprint spoofing" so that we reviewed the 180 most relevant results according to Google search engine. We found 224 video contents, mostly explaining how biometric technology can be spoofed. Looking at the image results for this phrase, we found that there was no significant difference from the images we saw for the previous phrase.

The Google search engine results showed us that printed fingerprint images and fakes made of gelatin, latex, or other materials were the most common when using the listed phrases. Overall, we found that materials for making molds and materials for casts play a very important role in fingerprinting. This is important because a suitable material for molds must have structures that can mimic the ridges of the human fingerprint. After all, Henry Faulds, one of the modern founders of fingerprint recognition, has found differences in the fingerprints of people left in clay during archeological excavations. On the other hand, the material for casts must also have structures that go very easily into every pore of the mold. So, this means that in most cases materials in liquid state have better abilities to imitate human fingerprint. Sometimes it is possible to use material for molds also for materials for casts and vice versa. A detailed description of molds and casts and the results of making fingerprints can be found in the work of Kauba et al [20]. Encyclopedia of Biometrics also contains information on molds and casting materials and is a good source of information on the production of fake fingerprints [17].

5. RESEARCH RESULTS AND OUR METHOD FOR FABRICATION FAKE FINGERPRINT

In this research, we have tried to make a fingerprint that can unlock all the above biometric sensors used in mobile phones. Our primary goal was to successfully outsmart the ultrasonic fingerprint sensor. First, we started with known forms that we noticed while researching the current state of fingerprint spoofing methods.

So, we used clay, wax, latex milk, Play-Doh, and Kiddy-Dough as molds. Latex milk was used for casts. Latex milk proved to be the best material for casts because it can form a thin film on the mold and penetrates every pore of the mold very easily.

The procedure for making the cast was as follows. A finger is gently pressed into the mold and also gently withdrawn from the mold. Latex milk is then applied with a brush.

After one to two hours of drying time, which depends on how thin the layer of latex milk in the mold is, the fake fingerprint can be gently pulled out of the mold.

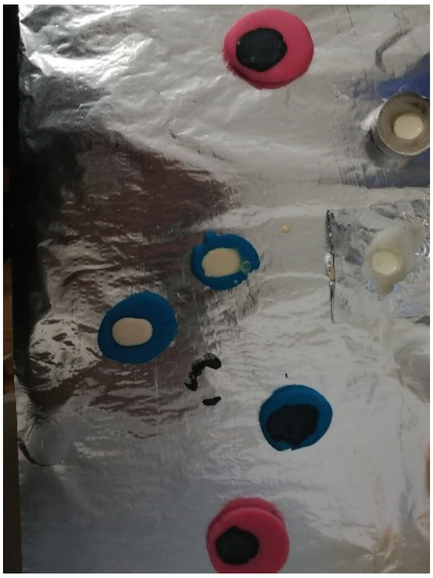

***Figure 2** Latex milk in molds*

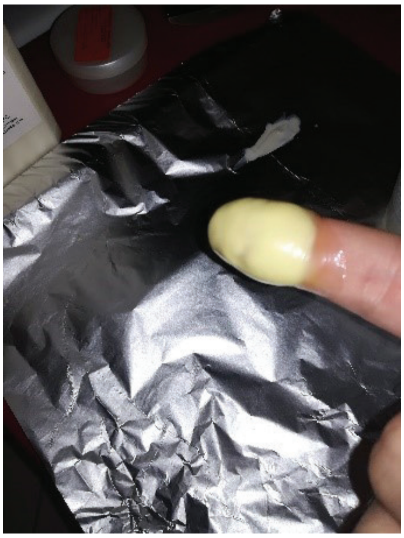

***Figure 3** Mold from latex milk*

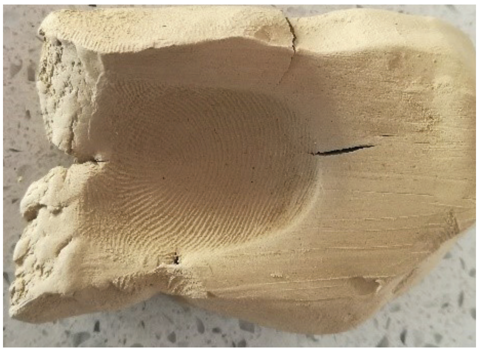

***Figure 4** Mold from clay*

Figure 2. shows different materials that were used for the mold and the prints inside it. White molds were made from wax, blue molds from modeling clay, and pink molds from Kiddy Dough. The casts were made from latex milk and latex milk mixed with graphite powder (black color of the casts) to maintain the conductivity of the material. In Figure 3. latex milk was used for the mold and in Figure 4. clay was used for the mold. Table 2. summarizes our observations.

Our conclusions were as follows. Wax, Play-Doh, Kiddy-Dough were good materials for molds, as was clay. Using latex for molds is not a good solution because it is better to use less liquid materials for molds or materials that dry very quickly, for example three or four minutes. If you have your finger in the material for molds for several hours (drying latex is a process that takes time depending on the thickness of the material, and for molds it is always better if the material is thicker), it is almost impossible to make fingerprint.

As can be seen from Figure 2. only latex milk and latex milk mixed with graphite powder were used for casts. Latex milk is a good material for casts because it has all the properties mentioned in the previous sections and chapters. We found that latex milk has a much longer drying time than the other materials. This means that this material is not completely dry when it is pulled out after at least 1 hour. This property of the material is desirable because there is a conductivity of the material which is necessary when we are dealing with touch screens or capacitive sensors. It is known that latex milk belongs to the group of polymers that are good insulators, so when this material becomes dry, there is less chance that fake fingerprints will affect the sensors. As a reminder, optical and ultrasonic sensors are located under the touch screens in mobile phones and for any interaction with them it is necessary to activate the touch screens. Considering this fact, we mixed latex milk with graphite powder. This is also a well-known solution presented in methods for making fake fingerprints described everywhere in the literature. Having made several fake fingerprints with latex milk mixed with graphite powder, we express doubts about the effectiveness of this method.

***Table 2.** The time required to produce the mold*

MATERIAL FOR MOLD	TIME AFTER FINGER COULD BE PULLED OUT FROM MOLD	TIME NEEDED THAT MOLD BE PREPARED FOR USE
Clay	Immediately	At least 24 hours
Wax	After 5 – 10 minutes. The process can be accelerated if the finger and wax immerse in cold water.	5 – 10 minutes.
Play-doh	Immediately	There is no need for drying
Kiddy-dough	Immediately	There is no need for drying
Latex	At least 25 minutes but it depends on thickness.	At least 1 hour

First, after these prints dried in the sense that they no longer contained moisture, they also had insulating properties. Secondly, and more importantly, the graphite powder mixed in the milk caused the porosity of the material, so that the ridges in the casts could be damaged. Due to these facts, we have abandoned this way of making fake fingerprints.

Another important thing about making casts for fake fingerprints is that you have to be sure that the latex milk is dry enough to be pulled out. This is important because if the fake fingerprints are not dry enough, their structure can be damaged when they are pulled out, and also when they are applied to the sensor combs, they can be damaged. This makes them unable to imitate the originals. This damage is barely visible to the naked eye.

For testing fake fingerprints, we decide to use a scale with the following values: successful, unsuccessful and partially successful. Successful here means that we fooled a particular type of sensor with any fake fingerprint, unsuccessful means that we did not fool any particular sensor and partially successful means that we fooled a particular sensor after several attempts with some fake fingerprints but not always the same one. The phones we used are listed in Table 1. The results of our tests can be seen in Table 3.

From the knowledge we gained from making the fingerprints, we realized that to make a good imitation of the fingerprint, we need a better shape and a better impression. We had two principles that we wanted to fulfill:

1. the creation of a fake fingerprint must be a simple process with no room for error.

2. the fake fingerprint must be as similar as possible to the real fingerprint.

This second principle is especially important because of the new generation of sensors, e.g. 3D Sonic Qualcomm's sensor.

***Table 3.** Results of testing sensors in mobile phones using fake fingerprint*

MANUFACTURER	MODEL	SENSOR TECHNOLOGY	TESTING RESULTS
Samsung	S8	capacitive	partially successful
Samsung	S10+	ultrasound	unsuccessful
Samsung	S20	ultrasound	unsuccessful
Huawei	P10 lite	capacitive	partially successful
Huawei	P30 Pro	optical	partially successful

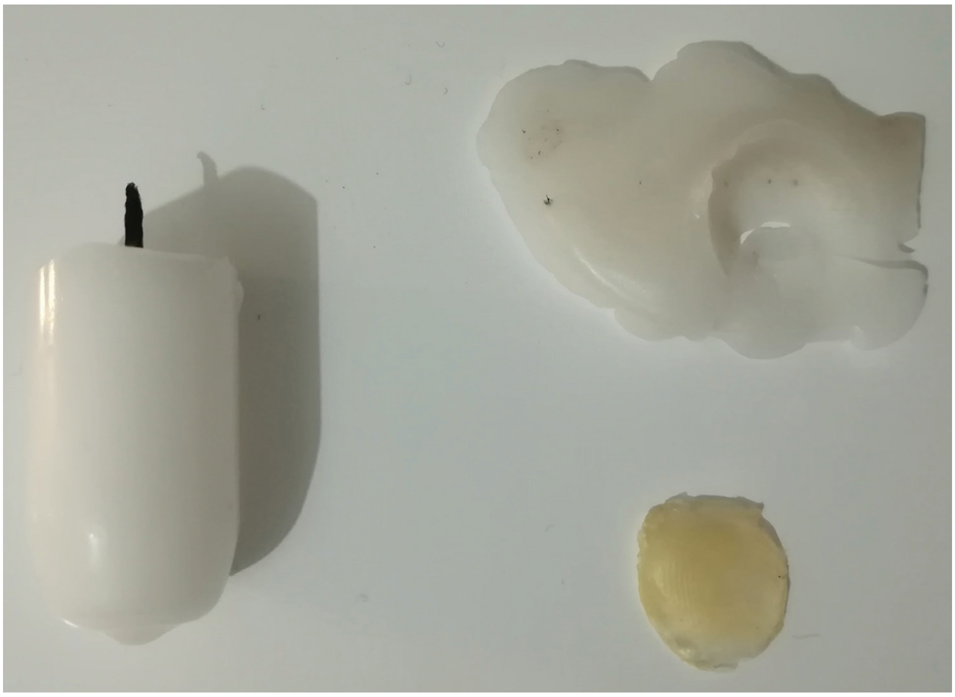

***Figure 5** Successful fingerprint casts from wax mold*

Moreover, there are articles in web magazines, which are among the top 500 most popular websites [21], where it is claimed that the ultrasonic sensor cannot be fooled by a fake fingerprint or synthetic skin [22].

Following the mentioned principles, we decided to use alginate for the mold and for the casts we did not find any material that is cheaper, more available and with better properties than latex milk. Alginate is a well-known material often used in dental practice and by artists who create sculptures with highly visible details, such as wrinkles on human skin.

It took only five minutes to make a mold with alginate (see extended results in Table 4). After the mold was ready, we placed it in latex milk (see Figure 6). The process of drying the latex milk took 24 hours (see Figure 7). After the impression was taken, a human finger was produced with identical folds and ridges as a real finger (see Figure 8).

In Figure 8. there are four fingerprints. The first (from the left) was made one month before the other three. The latex milk has dried completely and this print had 2 grams less than when it was removed from the mold (it weighed 9 grams).

***Table 4.** The time required to produce and use alginate mold*

MATERIAL FOR MOLD	TIME AFTER FINGER COULD BE PULLED OUT FROM MOLD	TIME NEEDED THAT MOLD BE PREPARED FOR USE
Clay	Immediately	At least 24 hours
Wax	After 5 – 10 minutes. The process can be accelerated if the finger and wax immerse in cold water.	5 – 10 minutes.
Play-doh	Immediately	There is no need for drying
Kiddy-dough	Immediately	There is no need for drying
Latex	At least 25 minutes but it depends on thickness.	At least 1 hour
Alginate	4 minutes	4 minutes

Table 5. *Results of testing sensors in mobile phones using fake fingerprint made with alginate mold and latex milk*

MANUFACTURER	MODEL	SENSOR TECHNOLOGY	TESTING RESULTS
Samsung	S8	capacitive	successful
Samsung	S10+	ultrasound	successful
Samsung	S20	ultrasound	successful
Huawei	P10 lite	capacitive	successful
Huawei	P30 Pro	optical	successful

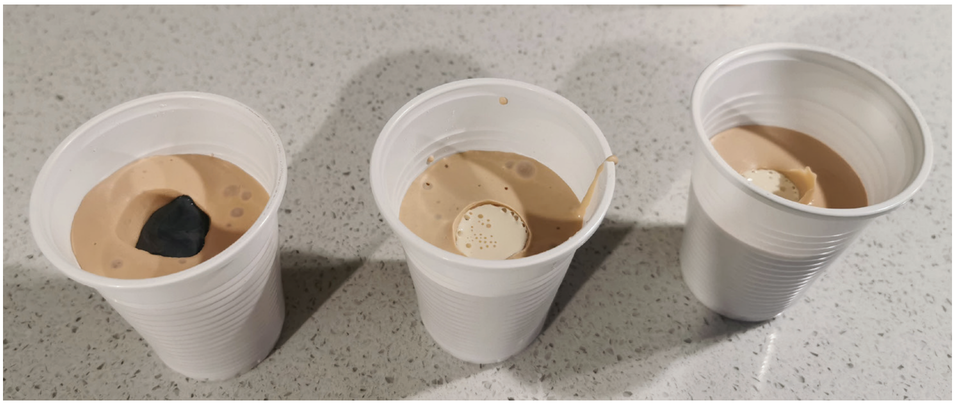

Figure 6 *Alginate molds with infused latex milk*

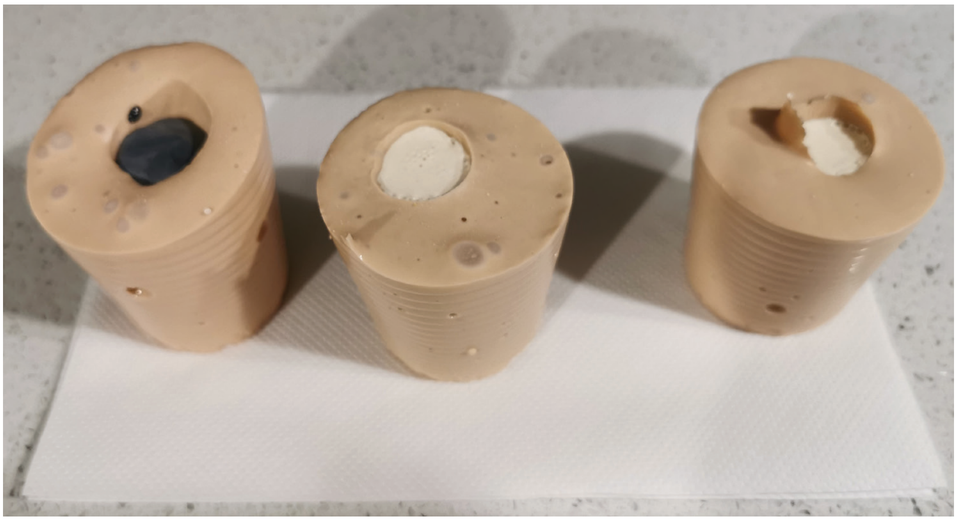

Figure 7 *Process of drying casts*

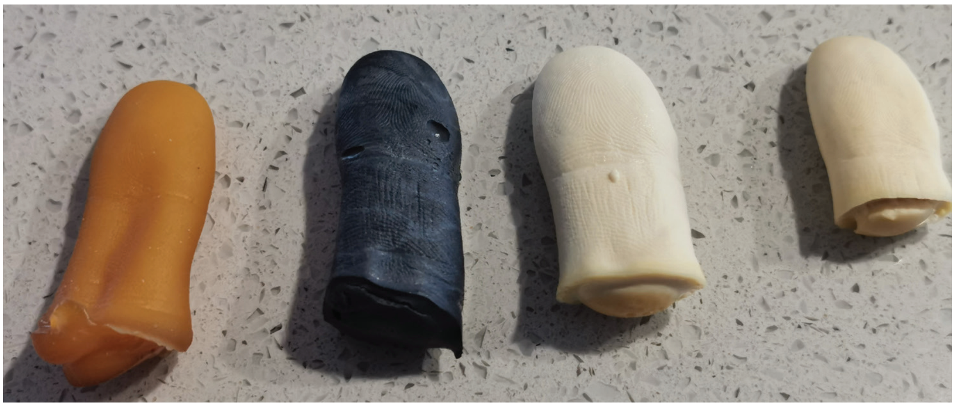

Figure 8 *Fabricated fingerprints with alginate mold and latex milk*

It was completely unusable because the ribs were deformed and the material became a complete insulator. Later, we found a way to preserve the latex fingerprint so that it would be kept in water or a water-based lubricant all the time. The second fingerprint (the black one) was made from latex milk mixed with graphite powder and was also unusable because the graphite particles damaged the ridges (this can be seen in the picture). The last two fake fingerprints were fully functional and successfully fooled any cell phone sensor (see Table 4). For testing, we used the same scale we described earlier and the same mobile phones listed in Table 1.

The results can be seen in Table 5.

The sensors were already fooled on the first or second attempt. We could not find any difference between the sensor types, which would indicate that one technology is better than the other.

6. CONCLUSION

As a consequence of the research results, it was concluded that protecting various confidential data on mobile phones only by biometric fingerprint sensors is not sufficient. More complex authentication is required. We have shown that it is very easy to make a fake fingerprint. Alginate has proven to be a very good molding material. It is also an available material that can be purchased at hobby art stores. The same facts apply to latex milk. So, both materials, for molds and for casting, satisfy our first principle of making false fingerprints. Our second principle is also satisfied, since we have successfully imitated the human fingerprint as far as is possible with readily available materials. Based on the success we have had in fooling sensors, we can propose our method of making fake fingerprints as the standard in testing fingerprint sensors for their ability not to be fooled.

7. REFERENCES

[1.] J. Andress, The Basic Information of Information Security. Syngress Press, 2011., ISBN: 978-1-5974-9653-7

[2.] F. Schneider, “CS 513 System Security -- Something You Know, Have, or Are.” https://www.cs.cornell.edu/courses/cs513/2005fa/NNLauthPeople.html (accessed Feb. 07, 2021).

[3.] M. Kücken and A. C. Newell, “Fingerprint formation,” J. Theor. Biol., vol. 235, no. 1, pp. 71–83, 2005, doi: 10.1016/j.jtbi.2004.12.020.

[4.] D. Maltoni Davide; Maio, Handbook of Fingerprint Recognition. 2009. ISBN: 978-1848822689

[5.] Guodong Guo and H. Wechsler, Mobile biometrics. 2017. ISBN: 978-1-7856-1095-0

[6.] A. K. Jain, A. A. Ross, and K. Nandakumar, Introduction to Biometrics. 2011. ISBN 978-0-3877-7325-4

[7.] M. Gao, X. Hu, B. Cao, and D. Li, “Fingerprint sensors in mobile devices,” Proc. 2014 9th IEEE Conf. Ind. Electron. Appl. ICIEA 2014, pp. 1437–1440, 2014, doi: 10.1109/ICIEA.2014.6931394.

[8.] “In-display Fingerprint Sensors: Types and Working.” https://circuitdigest.com/article/in-display-fingerprint-sensors (accessed Feb. 12, 2021).

[9.] “Press Release | FS9100 Fingerprint Sensor | Synaptics.” https://www.synaptics.com/company/news/fs9100-optical-fingerprint-sensor (accessed Feb. 17, 2021).

[10.] I. E. T. S. Series, Information Security Foundations, technologies and applications. IET The Institution of Engineering and Technologies, 2018. ISBN: 978-1-8491-9974-2

[11.] B. W. An, S. Heo, S. Ji, F. Bien, and J. U. Park, “Transparent and flexible fingerprint sensor array with multiplexed detection of tactile pressure and skin temperature,” Nat. Commun., vol. 9, no. 1, pp. 1–10, 2018, doi: 10.1038/s41467-018-04906-1.

[12.] “Capacitive sensing - Wikipedia.” https://en.wikipedia.org/wiki/Capacitive_sensing (accessed Feb. 17, 2021).

[13.] "Qualcomm 3D Sonic Sensor: ultrasonic security solution I Qualcomm." https://www.qualcomm.com/products/features/fingerprint-sensors (accessed Feb. 17, 2021).

[14.] "Synaptics releases optical fingerprint sensors for smartphones | Biometric Update." https://www.biometricupdate.com/201612/synaptics-releases-optical-fingerprint-sensors-for-smartphones (accessed Feb. 17, 2021).

[15.] "Introducing Qualcomm 3D Sonic Sensor Gen 2." https://www.qualcomm.com/news/onq/2021/01/11/introducing-qualcomm-3d-sonic-sensor-gen-2 (accessed Feb. 17, 2021).

[16.] "Mobile Vendor Market Share Croatia | StatCounter Global Stats." https://gs.statcounter.com/vendor-market-share/mobile/croatia (accessed Feb. 17, 2021).

[17.] A. K. Li, Stan Z. Jain, Ed., Encyclopedia of Biometrics. 2015., Second Edition, ISBN: 978-1-4899-7489-1

[18.] "'fingerprint spoofing' - Google pretraživanje." https://www.google.com/search?q=%22fingerprint+spoofing%22&source=lmns&bih=937&biw=1920&hl=hr&sa=X&ved=2ahUKEwiQ0_-t4OnuAhWF-KQKHYooDGcQ_AUoAHoECAEQAA (accessed Feb. 14, 2021).

[19.] "'fake fingerprint' - Google pretraživanje." https://www.google.com/search?q=%22fake+fingerprint%22&hl=hr&sxsrf=ALeKk00edMjQPqfhQBOCFm-CnEtanP1QRA:1613333415602&ei=p4MpYPbsI8KprgSktq_wDg&start=0&sa=N&ved=2ahUKEwi23I-pl-ruAhXClIsKHSTbC-44ChDy0wN6BAgEEDg&biw=1920&bih=937 (accessed Feb. 14, 2021).

[20.] C. Kauba, L. Debiasi, and A. Uhl, "Enabling fingerprint presentation attacks: Fake fingerprint fabrication techniques and recognition performance," arXiv, pp. 1–23, 2020.

[21.] "Top 500 Most Popular Websites - Moz." https://moz.com/top500 (accessed Feb. 19, 2021).

[22.] "Galaxy S10 has an ultrasonic fingerprint scanner. Here's why you should care - CNET." https://www.cnet.com/news/galaxy-s10-has-ultrasonic-fingerprint-scanner-heres-why-you-should-care-explainer/ (accessed Feb. 17, 2021)

[23.] M. Žagar, K. Pukšić, "Security of biometric security systems based on fingerprint authentication", 2016., Polytechnic and Design, doi: 10.19279/TVZ.PD.2016-4-3-16

AUTHORS

● Domagoj Tuličić

Rođen je 07.02.1977. godine u Zadru. U Zagrebu je završio gimnaziju Tituša Brezovačkog, a 2007 diplomirao je na Sveučilište u Splitu - Stručni studij računarstva – smjer programer te je stekao zvanje inženjera. Dana 7.12.2018. godine na Sveučilište u Zagrebu – Fakultet organizacije i informatike – smjer Baze podataka i baze znanja stekao je diplomu magistra informatike. Iste godine na Fakultetu organizacije i informatike upisuje doktorski studij. Od 2003. godine radi isključivo na poslovima i radnim zadacima vezanim uz primjenu informatičke tehnologije. Prvo zaposlenje je u vlastitom obrtu od 2003 do 2008 na poslovima programera kao i na svim ostalim poslovima koji su nužni u vođenju vlastitog obrta. U tvrtki Kor d.o.o. 2007 godine radio je kao SQL programer na Microsoft SQL bazi podataka. Od 2008 – 2018 godine bio je zaposlenik Državne uprave za zaštitu i spašavanje (DUZS), gdje je radio kao nadzornik za programsku podršku i izradu baza podataka. Tijekom ovog perioda radio je na izradi izvještaja o incidentima u RH, izradi nekoliko bitnih sustava za zaštitu i spašavanje u RH, kao i na međunarodnom projektu „Next Generation Incident Command System" u kojem je surađivao s Massachusetts Institute of Technology Lincoln Laboratory. Od 1. veljače 2018 godine do danas radi na Tehničkom veleučilištu u Zagrebu kao asistent.

Correspondence
domagoj.tulicic@tvz.hr

● Marinko Žagar - biograpgy can be found in the Polytechnic & Design Vol. 4, No. 1, 2016.

Correspondence
marinko.zagar@tvz.hr