IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol-6, Special Issue-6, July 2018 E-ISSN: 2347-2693

Bypass Mobile Lock Systems With Gelatin Artificial Fingerprint

E.A. Maro[1*], M.M. Kovalchuk[2]

[1,2]Dept. of Information Security, Institute of Computer Technologies and Information Security, Southern Federal University, Taganrog, Russia

[*]*Corresponding Author: eamaro@sfedu.ru, Tel.: +7-8634-371905*

Available online at: www.ijcseonline.org

***Abstract*—** We briefly described how to bypass mobile devices lock system by using fingerprint verification. As the applying method the method of counterfeiting the fingerprint of the mobile device's owner was chosen (direct attack). The article describes the use of the method of creating a gelatin artificial fingerprints to bypass the locking system of mobile phones. The experiment confirmed the possibility of bypassing fingerprint protection without the need for expensive tools or high-quality fingerprint samples. The artificial fingerprints were tested to unlock iPhone 6 and Meizu m5s phones. To bypass lock system the iPhone 6 with a fake fingerprint we need not more than two unlock attempts. Success rate of bypass iPhone 6 biometric lock system was 70 percent. To unlock Meizu m5s we have to moistening the artificial fingerprint, after that we bypass lock system with the first unlock attempt. Success rate of bypass Meizu m5s biometric lock system was 70 percent.

***Keywords*—** Biometric security systems, Fake artificial fingerprints, Mobile fingerprint readers, Gelatin fingerprint copy.

I. INTRODUCTION

It is generally known that fingerprints of each person are unique and there are not two identical ones. Nevertheless, there are ways to bypass biometric authentication systems built on fingerprint verification [1-13]. Mobile phones and other electronic devices with fingerprint readers are not as secure as it is commonly believed [14-24].

The main problem of fingerprint authentication systems is that if someone steal your fingerprints or get access to the fingerprint database, we can not change them anymore – unlike a password that can be update immediately.

In this article we will consider the process of obtaining a fingerprint sample, as well as demonstrate the practical testing of the possibility of using a gelatin fingerprint to unlock the phones.

Rest of the paper is organized as follows, Section II contain the related work of bypass mobile fingerprint authentication systems, Section III contain the methodology of creating a gelatin artificial fingerprint, Section IV contain the experimental results of bypass mobile fingerprint authentication systems with gelatin artificial fingerprint, Section V concludes research work with future research directions.

II. BYPASS MOBILE FINGERPRINT AUTHENTICATION SYSTEMS

There are eight points or levels of attacks against biometric authentication systems (Figure 1.).

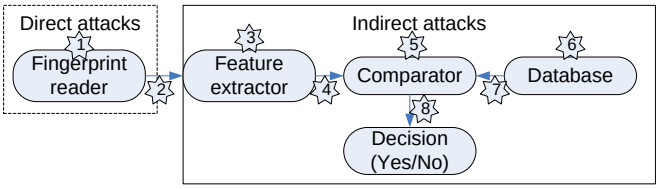

Figure 1. Fingerprint authentication system attacks.

Direct attacks consist of presenting artificial or fake biometric fingerprint samples to the fingerprint reader. This attack can be carried out as spoofing and alteration attacks. Spoofing attacks it is such attack, when someone presents a fake biometric sample (silicon finger, etc.) to the biometric reader in order to gain unauthorized access. Alteration attack based on modifications of standard biometric samples using obliteration, distortion, imitation or falsification.

Indirect attacks based on alteration the interface between authentication system modules or on the software modules.

The following directions of attacks on fingerprint-based authentication systems are exist:

— gain access to the database of fingerprints on devices (if database is not encrypted);
— creating a fake fingerprint (3D-printing [18-21], printing with conductive ink, latex, glue or gelatin fingerprint copy [17, 24], etc.);
— interception of fingerprint samples from fingerprint readers (man in the middle attack, SDK or API vulnerabilities, malware, fingerprint sensor spying attack, replay attack, etc.) [16, 22-24].

Paper [16] presents the first alteration attack on biometric mobile applications. This attack based on image trace using altered versions of reference images of the user in order to gain illegitimate access to biometric mobile applications.
Paper [22, 24] presents a security analysis of the mobile fingerprint authentication system and propose four different indirect attacks: the confused authorization attack that enables malware to bypass pay authorizations protected by fingerprints; insecure fingerprint data storage; fingerprint sensor exposed to the untrusted world; pre-embedded fingerprint backdoor.
Research [23] includes analysis of the fingerprint API in Android and prove that some app do not use this API in the most secure way.

Within the framework of our experiments we will consider direct attacks on biometric fingerprint authentication systems. Paper [17] proposed a simple, fast and effective method to generate 2D fingerprint spoofs that can successfully hack built-in fingerprint authentication in mobile phones. This attack has three main steps: get a user's fingerprint sample; print the fingerprint on a transparent sheet with a thick toner setting; create a "spoof fingerprint" using latex milk or white wood glue. Research [21] casts universal 3D fingerprint targets, which can be imaged on the three major fingerprint reader types in use (contact-optical, contactless-optical, and capacitive).

III. METHODOLOGY OF CREATING A GELATIN ARTIFICIAL FINGERPRINT

This section of the article describes the applied methodology for making a fingerprint for mobile devices and its use to unlock the device. In the conducted experiment iPhone 6 with protective glass and Meizu m5s phone were used.
The primary task is to get the original fingerprint of the owner of the phone. To obtain a sample of a typo of the owner of the iPhone 6, we unfasten the protective glass so as not to leave your fingerprints among the available ones. Then pour a little dactyloscopic powder on the surface of the protective glass with the alleged fingerprint of the phone's owner. As shown by experiments carried out to remove the fingerprint, the layer of dactyloscopic powder should be small: less than 2-3 millimeters (Figure 2).

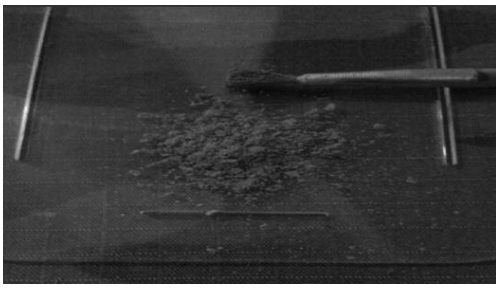

Figure 2. Dactyloscopic powder application.

Once the powder has been applied, it should be carefully and slowly distributed over the surface of the protective glass. After making several movements, you will see fingerprints of gray color. Finely dispersed powder adheres to the traces of fat and creates a visible image of the fingerprint. We spread it all with a soft brush, so as not to damage the papillary pattern (Figure 3).

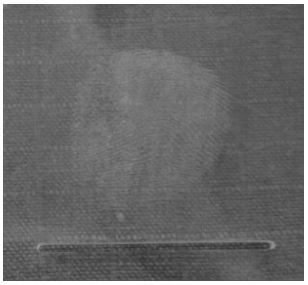

Figure 3. Visible fingerprint image on the surface of the protective glass.

In order to work with a fingerprint it is necessary to transfer it to a dactyloscopic film or we can use an ordinary scotch tape. We move out the film without excessive pressure, so as not to break the contours of the papillary pattern (Figure 4).

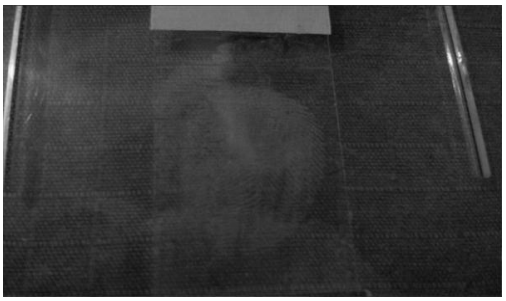

Figure 4. Move out fingerprint from the protective glass.

Do not pull too fast to not break the structure of the adhesive, we remove the film. If all the lines are clearly visible on a dactyloscopic film (scotch tape), then the removal of a fingerprint sample with a high probability was successful. Figure 5 shows the sample of the print on scotch tape.

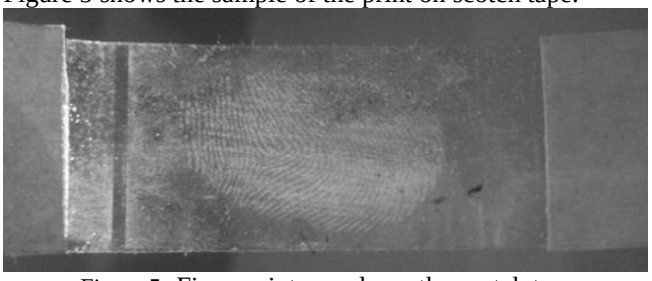

Figure 5. Fingerprint sample on the scotch tape.

We do not need a perfect fingerprint sample suited for further work with bypassing the phone lock (such sample can be taken without additional specialized tools).

The next step is to scan or photograph the resulting fingerprint with a resolution of at least 2400 dots per inch. Then with the help of the graphic editor the image is rotated along the vertical axis, the color of the image is inverted (the image is made white and the background is black), the contrast and sharpness are increased. The final processed image of the fingerprint is shown in Figure 6.

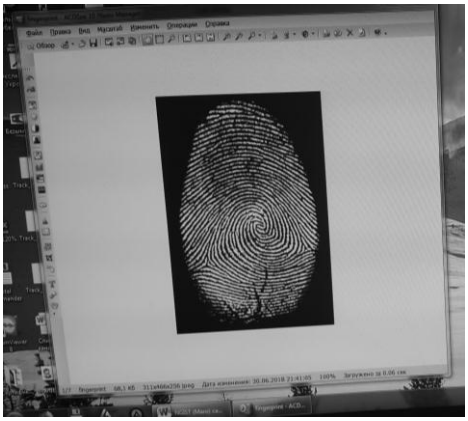

Figure 6. Final image of the fingerprint.

The third step of the applied method is to make a volumetric impression of the fingerprint. There are several ways how to make a convex mask and how to pour it to obtain an artificial fingerprint. We applied a method that requires the least amount of time and additional equipment for practical implementation. We make the artificial fingerprint on the printed image using the bulges of the laser printer's toner. During the experiments it was established that the printer settings should be set to the maximum print resolution (1200 DPI and more is recommended) and the maximum toner consumption.

Then fill the gelatin to a printed image and place it in the refrigerator to freeze for about 10 minutes at +4ºC. After gelatin takes the state of the rubber we carefully remove the gelatin mold from the paper. To obtain the final fingerprint, we cut off the unnecessary edges of the artificial fingerprint. As a result we get an artificial fingerprint suitable for unlocking a mobile phone (Figure 7).

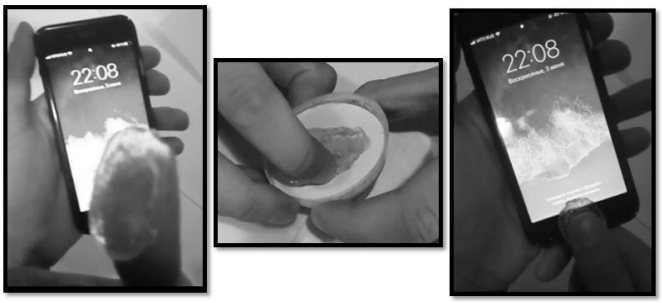

Figure 7. Gelatin artificial fingerprint.

IV. EXPERIMENTAL RESULTS

iPhone uses protection from fingerprint brute force attack: after five incorrect unlock attempts we cannot unlock the phone with a fingerprint and we will need to unlock it with the password. In our research it is important to prevent the unlocking process with the password, so that the work done was not in vain. In the experiment we managed to bypass the iPhone lock with an artificial fingerprint. The fingerprint reader on the iPhone 6 on the second attempt took the artificial fingerprint as valid fingerprint and unlocked the phone.

Unlocking of the Meizu m5s phone using an artificial print was more difficult. The fingerprint reader of Meizu m5s did not perceive the artificial fingerprint. It was concluded that the fingerprint reader does not respond to the dry artificial fingerprint. We unlocked the Meizu m5s phone after moistening the artificial fingerprint to simulate the sweat by the first attempt.

The results of conducted experiments to bypass the blocking of mobile phones are given in Table 1.

We should note that the applied method is not suitable for fingerprint readers, in which the electrical conductivity of the skin is measured. Gelatin fingerprint can be stored for a long time if the storage conditions are kept (keeping the fingerprint in the low temperature). If we do not comply with the storage conditions, the artificial fingerprint will become unusable: gelatin may begin to melt and capillaries that are scanned by the fingerprint reader will deform.

Table 1. Experiments result to bypass the blocking of mobile phones

Phone model	**Parameters of artificial fingerprint**	**Number of unlock attempts**	**Number of successful unlock attempts**	**True positive rate (%)**
iPhone 6	Original artificial fingerprint	20	14 (70%)	70
Meizu m5s	Original artificial fingerprint	10	does not perceive as a fingerprint	-
	Moistening artificial fingerprint	20	13	65

The thickness of the gelatin layer on fingerprint's printed copy was approximately 3-4 mm. Thickness control was carried out manually, we put gelatin solution drop by drop onto the fingerprint copy. In the experiments thickness of the gelatin layer did not directly affect to acceptance of fingerprint as valid. However significant excess of fingerprint's thickness (more than 1 cm) caused difficulties with apposition an artificial fingerprint to the reader, in this case we carefully trimmed reverse side of the artificial fingerprint to the required thickness.

In the research our main tasks were experimentally testing of direct attacks approach to mobile devices biometric lock systems and debugging of implementing attack technique. In prospect, of course, it is necessary to expand the field of research and estimate probability of false positives rate on a set of artificial fingerprints.

V. CONCLUSION

The presented results are the beginning of research in the field of biometric fingerprint authentication. Future scope for improvement research includes extension of the list of devices for which we check the unlock possibility with gelatin artificial fingerprint. Also we plan to use other technologies for creating artificial fingerprint, for example, 3D printing and printing with conductive ink.

Summing up the experiments we note that fingerprints can be recommended for use on smart phones, notebooks and other devices, but keep in mind that a fingerprint can be less reliable than a long password or PIN. More reliably way is use fingerprints as an additional factor for entering to important services or to unlock devices (combine fingerprint with password, hardware devises, etc). To increase the security of the biometric fingerprint authentication system we recommend:

- use several biometric samples (register several fingerprints of different fingers and perform fingerprint checks in random order);
- use of multifactor authentication systems (for example, fingerprint plus password or fingerprint plus SD-card);
- use of multimodal biometrics (for example, fingerprint plus scanning the iris or fingerprint plus face recognition);
- apply live finger detection technology: sensors with real-time ability to determine if the biometric characteristics presented to a fingerprint reader are genuine and not fake.

REFERENCES

[1] Olaf Henniger, Dirk Scheuermann, and Thomas Kniess "*On security evaluation of fingerprint recognition systems*", International Biometric Performance Conference (IBPC 2010), March. 2010.

[2] Javier Galbally, Julian Fierrez, and Javier Ortega-Garcia "*Vulnerabilities in Biometric Systems: Attacksand Recent Advances in Liveness Detection*", Proc. Spanish Workshop on Biometrics, SWB, 2007.

[3] Umut Uludag, Anil K. Jain "*Attacks on Biometric Systems: A Case Study in Fingerprints*", Proceedings of SPIE - The International Society for Optical Engineering, 2004.

[4] Swapnali Mahadik, K Narayanan, D V Bhoir, Darshana Shah "*Access Control System using Fingerprint Recognition*", *International Conference on Advances in Computing Communication and Control*, pp. 306-311, 2009.

[5] A. Nagar K. Nandakumar A. K. Jain "*Biometric template transformation: a security analysis*", IS&T/SPIE Electronic Imaging. International Society for Optics and Photonics, 2010.

[6] S. Yoon J. Feng A. K. Jain "*Altered fingerprints: Analysis and detection*", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34 no. 3 pp. 451-464 2012.

[7] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar "*Handbook of Fingerprint Recognition*", Springer, Berlin, Germany, 2009.

[8] "*Politician's fingerprint 'cloned from photos' by hacker*", December 2014, http://www.bbc.com/news/technology-30623611.

[9] T. van der Putte and J. Keuning "*Biometrical fingerprint recognition: don't get your fingers burned*", Proceedings of the 4th Working Conference on Smart Card Research and Advanced Applications, pp. 289–303, 2000.

[10] A. Nagar, K. Nandakumar, and A. K. Jain "*Biometric template transformation: a security analysis*", Proceedings of the SPIE, Electronic Imaging, Media Forensics and Security II, vol. 7541, San Jose, Calif, USA, January 2010.

[11] Rubal Jain and Chander Kant "*Attacks on Biometric Systems: An Overview*", International Journal of Advances in Scientific Research 2015, 1(07), pp. 283-288.

[12] Galbally, J., Fierrez, J., Rodriguez-Gonzalez, J.D., Alonso-Fernandez, F., Ortega-Garcia, J., Tapiador, M. "On the vulnerability of fingerprint verification systems to fake fingerprint attacks", Proc. of IEEE International Carnahan Conference on Security Technology. Volume 1. (2006) 130–136.

[13] E. Marasco and A. Ross "*A Survey on Anti-Spoofing Schemes for Fingerprint Recognition Systems*",ACM Computing Surveys, Vol. 47, No. 2, Article 28, January 2015.

[14] White Paper "*Protecting Against Fingerprint Spoofing in Mobile Devices*", Synaptics Incorporated, 2016.

[15] Y. W. Ju B. H. Lee "*The implementation of secure mobile biometric system*", International Journal of Bio-Science and Bio-Technology , vol. 5 no. 4 pp. 53-60 2013.

[16] Sanaa Ghouzali, Maryam Lafkih, Wadood Abdul, Mounia Mikram, Mohammed El Haziti, and Driss Aboutajdine "*Trace Attack against Biometric Mobile Applications*", Mobile Information Systems, vol. 2016.

[17] Kai Cao and Anil K. Jain "*Hacking Mobile Phones Using 2D Printed Fingerprints*", MSU Technical Report MSU-CSE-16-2, 2016.

[18] S. S. Arora, K. Cao, A. K. Jain, and N. G. Paulter "*Design and fabrication of 3d fingerprint targets*", IEEE Transactions on Information Forensics and Security, vol. 11, pp. 2284–2297, Oct. 2016.

[19] S. S. Arora, A. K. Jain, and N. G. Paulter "*3d whole hand targets: Evaluating slap and contactless fingerprint readers*", 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1–8, Sept 2016.

[20] S. S. Arora, A. K. Jain, and N. G. Paulter "*Gold fingers: 3d targets for evaluating capacitive readers*", IEEE Transactions on Information Forensics and Security, pp. 1–1, Apr. 2017.

[21] Joshua J. Engelsma, Sunpreet S. Arora, Anil K. Jain, Nicholas G. Paulter Jr. "*Universal 3D Wearable Fingerprint Targets: Advancing Fingerprint Reader Evaluations*", IEEE Transactions on Information Forensics and Security, 2017.

[22] Yulong Zhang, Zhaofeng Chen, Hui Xue, and Tao Wei "*Fingerprints On Mobile Devices: Abusing and Leaking*", Black Hat Conference, August 7, 2015.
[23] Antonio Bianchi, Yanick Fratantonio, Aravind Machiry, Christopher Kruegel, Giovanni Vigna, Simon Pak Ho Chung, Wenke Lee "*Broken Fingers:On the Usage of the Fingerprint API in Android*", Network and Distributed System Security Symposium (NDSS), February 19th, 2018.
[24] Yulong Zhang, Tao Wei "*To Swipe or Not to Swipe: A Challenge for Your Fingers*", RSA conference, San Francisco, USA, 2015.

Authors Profile

Dr. Ekaterina Maro was graduated from Southern Federal University (SFedU), Russia, Taganrog in 2009. She is currently working as Assosiate Professor in Department of Information Security, Institute of Computer Technologies and Information Security, Southern Federal University. She has about 41 publications in Russian and foreign, 7 of which are published in journals recommended by the Higher Attestation Commission to reflect the main content of candidate and doctoral dissertations; 5 articles are included in the citation system Scopus and Web of Science. Dr. Maro was a member of the organization committee of The International Conference "Security of information and networks" (http://sinconf.org) (2010-2017), The International Conference "Intelligent Communication and Computational Techniques", ICCT'17, The International Conference "Next Gen Information Systems and Technologies". Her main research work focuses on Information Security Systems, Cryptography, Cryptanalysis, Symmetric Block Ciphers, Algebraic Analysis, Boolean Systems of Equations. She has 7 years of teaching experience and 9 years of research experience.

Mr Maxim Kovalchuk is Bachelor of Information security third course student on Department of Information Security, Institute of Computer Technologies and Information Security, Southern Federal University. He is currently working at research project on the analysis of the reliability of biometric authentication methods. His main research work focuses on Information Security, Biometric Systems of Authentication and Security of Mobile. He presented his research reports at the studetn's workshops and conferences at Southern Federal University.

