Gummy and Conductive Silicone Rubber Fingers
— Importance of Vulnerability Analysis —

Tsutomu Matsumoto

Yokohama National University
Graduate School of Environment and Information Sciences
79-7 Tokiwadai, Hodogaya, Yokohama 240-8501, Japan
tsutomu@mlab.jks.ynu.ac.jp

Abstract. Vulnerability evaluation of various biometric systems should be conducted and its results should be available to potential users.

Summary

Biometrics is utilized in individual authentication techniques which identify individuals by checking physiological or behavioral characteristics, such as fingerprints, faces, voice, iris patterns, signatures, etc. Biometric systems are said to be convenient because they need neither something to memorize such as passwords nor something to carry about such as ID tokens [1]. In spite of that, a user of biometric systems would get into a dangerous situation when her/his biometric data are abused. For example, you cannot change your fingerprints while you can change your passwords or ID tokens when they are compromised. Therefore, biometric systems must protect the information for biometrics against abuse, and they must also prevent fake biometrics.

We focus on fingerprint systems since they have become widespread as authentication terminals for PCs or mobile terminals. A fingerprint system has an enrollment process and a verification process. In an enrollment process, the system captures finger data from an enrollee with sensing devices, extracts features from the finger data, and then record them as a template with a personal information, e.g. a personal identification number (PIN), of the enrollee into a database. We are using the word *finger data* to mean not only features of the fingerprint but also other features of the finger, such as *live and well* features. In a verification (or identification) process, the system captures finger data from a finger with sensing devices, extracts features, verifies (or identifies) the features by comparing with templates in the database, and then outputs a result as *Acceptance* only when the features correspond to one of the templates. Most of fingerprint systems utilize *optical* or *capacitive* sensors for capturing fingerprints. These sensors detect difference between ridges and valleys of fingerprints. Optical sensors detect difference in reflection. Capacitive sensors, by contrast, detect difference in capacitance. Some systems utilize other types of sensors, such as *thermal* sensors, *ultrasonic* sensors. In this study we examine fingerprint systems which utilize optical or capacitive sensors.

Potential threats caused by something like real fingers, which are called *artificial fingers*, should be crucial for authentication based on fingerprint systems. However, vulnerability evaluation against attacks using such artificial fingers has been rarely disclosed.

As researchers who are pursuing secure systems, we would like to discuss attacks using artificial fingers and conduct experimental research to clarify the reality. We report that

1. *gummy fingers*, namely artificial fingers that are easily made of cheap and readily available gelatin, were accepted by extremely high rates by 11 particular fingerprint devices with optical or capacitive sensors [2], and

2. *conductive silicone fingers*, namely artificial fingers that are made of silicone rubber filled with electrically conductive carbon black of 12%-16%, were accepted by extremely high rates by the same set of fingerprint devices except for two devices using optical sensors with seemingly color-checking ability [3].

We have used the molds, which we made by pressing our live fingers against them, or by processing fingerprint images from prints on glass surfaces, or by processing impression of inked fingers. We describe how to make the molds, and then show that the gummy fingers and conductive silicone fingers which are made with these molds, can fool the fingerprint devices.

The fact that gummy fingers which are easy to make with cheep and easily obtainable tools and materials can be accepted suggests review not only of fingerprint systems but also of biometric systems. This experimental study on the artificial fingers will have considerable impact on security assessment of biometric systems. Manufacturers and vendors of biometric systems should carefully examine security of their system against artificial clones. Also, they should make public results of their examination, which lead users of their system to a deep understanding of the security. We would like to discuss the effect of such a vulnerability analysis and how to disclose the information based on our experience and the responses we received [4].

References

[1] Jain, K.: Introduction to biometrics, in Biometrics: Personal Identification in Networked Society, The Kluwer Academic, International Series in Engineering and Computer Science, Jain, A. K., Bolle, R. and Pankanti, S. eds., Vol. 479, Chapter 1, pp. 1-41, 1999.

[2] Matsumoto, T., Matsumoto, T., Yamada, K., and Hoshino, S.: Impact of Artificial "Gummy Fingers" on Fingerprint Systems, Optical Security and Counterfeit Deterrence Techniques IV, Rudolf L. van Renesse, editor, Proceedings of SPIE Vol. 4677, SPIE – The International Society for Optical Engineering, pp.275-289, 2002.

[3] Endo, Y. and Matsumoto, T.: Can we make artificial fingers that fool fingerprint systems? – PartW–, Proc. of IPSJ for Computer Security Symposium, 2002.

[4] Matsumoto, T.: What will you do if you find a particular weakness of a security technology?, Journal of IEICE, Vol. 84, No.3, 2001.