Protecting Against Fingerprint Spoofing in Mobile Devices

Table of Contents

Executive Summary	1
Introduction	2
Faking Fingerprints	2
Anti-spoofing Technology	4
Conclusion	6

SentryPoint™

Executive Summary

Biometric forms of authentication are becoming increasingly popular in mobile devices. Passwords and PINs are being replaced by this convenient and more secure form of identification. Although biometric forms of identification provide a higher level of security, hacking and spoofing techniques are also becoming more sophisticated. There are anti-spoofing technologies that can help defend against such risks to protect mobile devices from threats.

This white paper discusses ways to protect against fingerprint spoofing in mobile devices and provides an overview of different ways biometric authentication can be hacked, as well as how anti-spoofing technologies can help defend against such threats.

Introduction

Biometric forms of authentication are more convenient than passwords and PINs, and have other advantages that enhance the security of mobile devices. But just like passwords and PINs, biometric forms of identity can also be hacked. For example, a photo or a recording can be used as a spoof of facial or voice recognition systems, and even fingers can be faked—all without the user's cooperation or awareness.

The ability to spoof fingerprints—something that was demonstrated immediately after Apple® first incorporated a fingerprint scanner in the iPhone® model 5S in 2013—became substantially easier with the advent of affordable 3D printers. There has been at least one case of a police department employing 3D printing in an attempt to spoof the fingers of a deceased victim and gain access to his smartphone, believing it might contain clues to his murder.

To defend against these biometric fakes, sensors are now incorporating anti-spoofing technology, such as a facial recognition system requiring the user to blink to prove "liveness" of the scan. Because fingerprints are the most common form of biometric authentication on mobile devices today, this article will focus on two aspects of fingerprint spoofing: the techniques hackers use to spoof fingerprints; and the ways device manufacturers can defend against these spoofs.

Faking Fingerprints

Like other data utilized for user authentication, fingerprint images are subject to electric hacks. Such a breach involves a hacker gaining access directly to a database that contains user access credentials, or infecting a network-attached PC with malware capable of uploading the data. These databases are targeted because, in addition to containing passwords, PINs and biometric images, they often contain other information about users, such as social security numbers, that are quite valuable on the black market.

A notorious breach in 2015 involved the electronic hack of a U.S. Office of Personnel Management database containing 21.5 million federal employee records. Among the records were some 5.6 million fingerprint images, including those from undercover agents. This created a serious problem because fingerprint scanning is used to gain access to secure government accounts and facilities, and unlike passwords and PINs, fingerprints cannot be changed after a breach is detected.

Local authentication

Electronic hacks can be avoided by eliminating the need for "shared secrets" that require access credentials to be stored in databases. Instead, local authentication can be used to keep confidential information secure on the device. Local authentication with passwords, PINs and/or fingerprints is commonly used for "unlocking" mobile devices. More recently, it has been used to authenticate access to online accounts, as well as to authenticate onsite transactions via local wireless communications.

With local authentication, the user's private credentials never leave the device, significantly limiting its potential exposure. Nevertheless, local forms of biometric authentication are still accompanied by threat models involving electronic hacks of the biometric data. For example, by hacking the link between the device's sensor and authenticating software, stolen biometric data can be substituted during a scan, much like a "man-in-the-middle" attack hijacks communications between two systems.

Physical hacks

The more likely threat to local forms of biometric authentication is the physical hack; in this case, the creation of a fake finger. Because physical hacks are limited to a single user and/or device, they are less tempting to hackers. But the threat must be taken seriously by both device manufacturers and users alike, because fake fingers are fairly easy to create using inexpensive tools and materials—with or without a 3D printer.

Creating a fake finger without a user's awareness or cooperation involves three basic steps:

1. Lift and scan a fingerprint in high resolution
2. Print a mirror image of the scan on a plastic laminate or other material suitable for creating the equivalent of a mold
3. Cast the finger from the printed image (the mold)

A suitable fingerprint can obviously be found on the user's mobile device itself. The image can then be scanned on an ordinary scanner (the higher the resolution, the better), processed on an ordinary PC, and printed on an ordinary printer. Materials used to create the cast are equally ordinary, and include wood glue, Play-Doh®, silicone and rubber. Suitable materials are also available for 3D printers. The fake finger can optionally be coated with a graphite powder or spray, or conductive ink or paint to make it more realistic (see Figure 1).

FIDO AUTHENTICATION

The FIDO® (Fast IDentity Online) Alliance is an industry consortium that has developed interoperable specifications for reducing the reliance on passwords to authenticate users of online services. Its Universal Authentication Framework (UAF) protocol specifies a "password-less" user experience for registering devices with online services. According to the FIDO Alliance, "Once registered, the user simply repeats the local authentication action whenever they need to authenticate to the service. The user no longer needs to enter a password when authenticating from that device. UAF also allows experiences that combine multiple authentication mechanisms such as fingerprint + PIN."

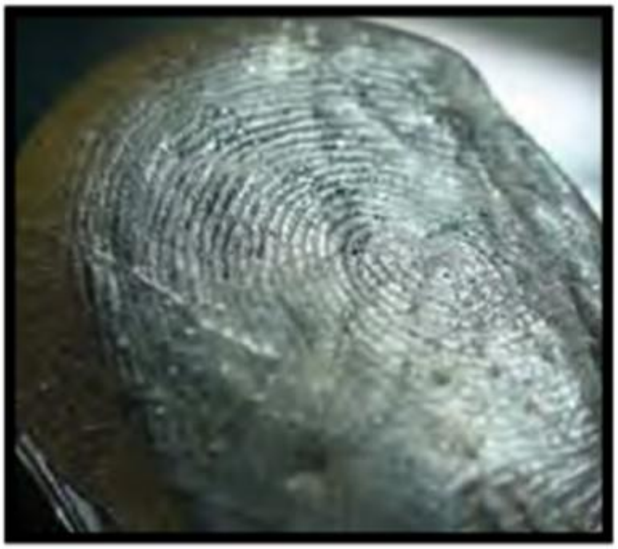

Figure 1: Fake finger cast with ordinary wood glue and coated with graphite powder

Fake fingers made this way can work on fingerprint scanners that lack robust anti-spoofing capabilities. Even better fakes can be made with the user's cooperation, which involves making the mold directly from the user's finger and not a lifted fingerprint. And it is these superior fakes that are often used for testing the effectiveness of anti-spoofing technology.

Anti-spoofing Technology

Advancements in technologies now afford sufficient protection against electronic hacks. For example, the Transport Layer Security (TLS) protocol can be used to encrypt communications between the sensor and the host to thwart interception. Even better protection is afforded by match-in-sensor technology where every scan is authenticated entirely within the sensor, which also securely contains the user's fingerprint enrollment used to make the match.

The current focus of anti-spoofing technology is, therefore, to detect when a fake finger is being used. As with any other technology, it is necessary to make tradeoffs in the design to balance device cost, anti-spoofing effectiveness and the user experience. For biometric authentication on mobile devices, this involves striking a prudent balance between "false rejects" (rejecting the user's actual finger) and "false accepts" (accepting a fake finger).

Anti-spoofing technology could be made 100 percent effective; that is, no fake finger would ever be accepted no matter how good the quality. But for a mobile device, such a solution would be very expensive and consume too much power, and the relatively high number of inevitable "false rejects" (all requiring rescans) would cause considerable user frustration and dissatisfaction.

Anti-spoofing technology employs many different techniques, but only one—liveness detection—currently has benchmark testing from an independent organization. LivDet (www.LivDet.org) sponsors Liveness Detection Competitions to evaluate the effectiveness of the anti-spoofing technology implemented in fingerprint and iris scanning solutions. LivDet also makes the benchmark test data available to device manufacturers to assist engineers in meeting the desired design goals for false reject and accept rates.

A common design goal is to have a false reject (or "live reject") rate of 0.35% and a false accept rate of about 6%. With these rates, a live finger will be rejected in about 1 in every 300 scans, and approximately 1 in every 16 fake fingers would be accepted. It is also common to use a "spoof reject" rate, which is the converse of the false accept rate; in this case, 94%. A highly secure design might have false reject and accept rates of 1.6% and 2% (98% spoof reject), respectively, while a "budget" design might use 0.15% and 10% (90% spoof reject) as its "good enough" objectives.

Software- versus hardware-based anti-spoofing technology

The anti-spoofing technology itself can be implemented in software, hardware, or both. Software-based solutions generally work by assessing characteristics of the sample, such as the sharpness of the lines and the presence of pores. Software has the advantage of being easier to implement and update, including over the air (OTA) as anti-spoofing techniques improve, much like anti-virus software gets updated with the discovery of new viruses. Software-based solutions are also better suited to employing machine learning where the technology is advancing quite rapidly.

Hardware-based solutions require additional capabilities in the fingerprint scanner, such as the ability to sense pulse, temperature, and capacitance, none of which can be done in software alone. Hardware has the advantage of greater ability to detect the "liveness" of the finger being scanned, but has the disadvantages of being more expensive, consuming more power and introducing latency if, for example, there is a need to sense multiple heartbeats.

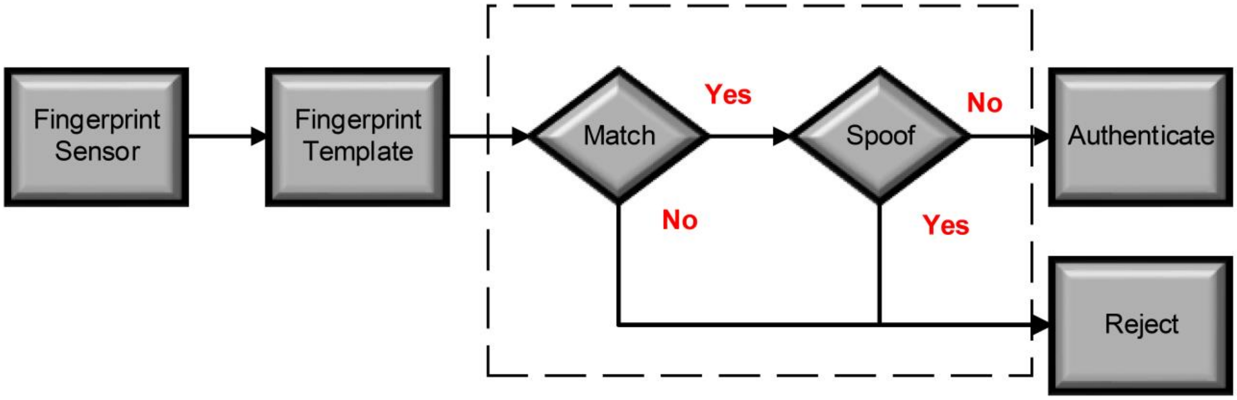

Figure 2: Matcher with Anti-spoof Engine

Conclusion

With the increased reliance on mobile devices for accessing online accounts and making onsite purchases, local authentication is taking on equally increased importance. Biometric forms of authentication are also becoming increasingly preferred for their greater convenience and other advantages over traditional usernames and passwords.

Juniper Research believes that the convenience, combined with the ubiquity of smartphones and the increasing use of near-field communications (NFC), will make biometric scanning a primary means of authenticating transactions. For these reasons, the firm predicts that the number of transactions authenticated by biometrics will increase from fewer than 130 million in 2015 to more than five billion by 2019.

As advancements in biometric authentication progress, so have the ability to create fake biometric images in order to spoof sensors built in mobile devices. To mitigate this risk, device manufacturers are now incorporating robust fingerprint anti-spoofing technology into their designs, and users are showing increased preference for these secure devices.

References

[1] FIDO Alliance: http://fidoalliance.org/

[2] Liv Det: http://livdet.org/

[3] Smith, Sam. *Apple Pay to Push Biometric Transactions to Nearly 5BN By 2019.* Juniper Research Ltd. http://www.juniperresearch.com/press/press-releases/apple-pay-to-push-biometric-transactions-to-nearly

Revision History

Table 1. Revision history

Revision	Reason for Change
A	Initial Release

Copyright

Trademarks

Synaptics; the Synaptics logo; SentryPoint; the SentryPoint logo are trademarks or registered trademarks of Synaptics Incorporated in the United States and/or other countries.

Apple and iPhone are trademarks of Apple Inc., registered in the U.S. and other countries. FIDO is a registered trademark of FIDO Alliance, Inc. All other trademarks are the properties of their respective owners.

Notice

Use of the materials may require a license of intellectual property from a third party or from Synaptics. This document conveys no express or implied licenses to any intellectual property rights belonging to Synaptics or any other party. Synaptics may, from time to time and at its sole option, update the information contained in this document without notice.

INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED "AS-IS," WITH NO EXPRESS OR IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES OF NON-INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS. IN NO EVENT SHALL SYNAPTICS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF THE INFORMATION CONTAINED IN THIS DOCUMENT, HOWEVER CAUSED AND BASED ON ANY THEORY OF LIABILITY, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, AND EVEN IF SYNAPTICS WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. IF A TRIBUNAL OF COMPETENT JURISDICTION DOES NOT PERMIT THE DISCLAIMER OF DIRECT DAMAGES OR ANY OTHER DAMAGES, SYNAPTICS' TOTAL CUMULATIVE LIABILITY TO ANY PARTY SHALL NOT EXCEED ONE HUNDRED U.S. DOLLARS

Contact Us

Visit our website at www.synaptics.com to locate the Synaptics office nearest you.