SentryPoint™ Encryption

PN: 507-000187-01 Rev. A

Table of Contents

Overview

Biometrics makes authentication easier for users, and more trustworthy for merchants and banks. But the use of biometric data also raises privacy and security concerns that can only be satisfactorily addressed with purpose-built protections.

Best practices, such as those promoted by the Fast IDentity Online (FIDO) Alliance principles, dictate that no biometric data should leave the device. However, it is necessary to create, process, and store biometric data *within* devices, including smartphones, tablets, PCs, and standalone biometric scanners. This white paper discusses how the potential vulnerabilities within a device can be minimized in all three states of biometric data:

- at rest: while stored;
- in process: when being modified; and
- in flight: when being moved.

Each state creates a different set of vulnerabilities and requires different measures to provide adequate privacy and security. To satisfy this need, the Synaptics SentryPoint™ security suite has been designed to minimize and, whenever possible, eliminate vulnerabilities in all three states, thereby providing the best available protection for biometric data.

While the many provisions of the SentryPoint security suite apply to all forms of biometric authentication, this white paper focuses on fingerprint sensing because it is the most widely-used form of authentication today.

Although SentryPoint is a comprehensive security suite, device manufacturers have the flexibility to choose which capabilities to implement to achieve the desired level of privacy and security—from a minimum level (to keep device cost low) to a maximum level (to provide the best possible protection).

The content of this white paper is limited to privacy and security protections within a device. There are numerous other provisions and protocols used to secure the end-to-end external communications that utilize user authentication (biometric or otherwise) to complete a transaction. Those topics are beyond the scope and intent of this document.

Match-on-Host versus Match-in-Sensor

While there are many functions involved in biometric forms of authentication, the most noteworthy is the “match” of the current scan with a known and secured template (a record of the user’s biometric identity). A positive match authenticates the user’s identity, permitting the transaction or access to proceed. A negative match might permit one or more additional attempts, but will ultimately result in the current transaction being terminated, and may even “lock” or disable the device. Some of the provisions needed to protect the privacy of the biometric data and to secure the integrity of the biometric authentication are, therefore, different depending on where the match is made: in the host’s CPU or in the biometric sensor IC(s). For this reason, the discussion in this white paper notes where any security provision is different between Match-on-Host and Match-in-Sensor.

Securing Data-at-Rest

Data-at-rest can be vulnerable to exploitation from malware infecting the host. Any tampering (such as the deleting or altering) with stored biometric data would cause user authentication to fail by preventing a definitive match, resulting in inconvenience and diminished confidence in the device. A much worse situation would exist if the biometric data could be used to produce a “false positive” match. But that would require moving and/or processing the data, so these vulnerabilities are covered in those sections.

The Synaptics SentryPoint security suite takes a layered approach, with robust provisions that protect the privacy of the user’s biometric data. This protection begins with the transformation of the biometric data during the scan into a proprietary “template” to ensure that the actual biometric data is never stored in the device.

The next layer of security involves the use of strong 256-bit Advanced Encryption Standard (AES) cryptography to prevent the user’s biometric template from being read by an unauthorized party or process, and the generation of a Message Authentication Code (MAC) to prevent injection, modification, or alteration of the biometric template.

SentryPoint also employs robust cryptographic key management provisions with single-use keys that are generated in hardware (the sensor IC) and are shared only with trustworthy processes as needed within the host’s Trusted Execution Environment (TEE). The specific techniques used to generate the session keys have passed rigorous testing established by the National Institute of Standards and Technology (NIST).

The final layer of data-at-rest security is determined by the choice of architecture. For Match-on-Host solutions, Synaptics recommends using either a secure area of system flash memory (good for most needs) or a dedicated flash memory module (a best practice). If the host lacks a means to secure data stored within its TEE, the use of dedicated memory is required. With the Match-in-Sensor architecture, all data-at-rest is stored entirely within this secure System-on-Chip (SoC) solution that contains a dedicated (private) flash memory module.

Securing Data-in-Process

In order to perform a match to authenticate the user during every transaction, biometric forms of authentication require other processes, such as enrolling the user's biometric template when the device is first used. These processes include one or more steps, which can be performed by the host's CPU and memory, by intelligence embedded in the biometric sensor IC(s), or by both, with the host and the sensor IC(s) each handling some of the steps. Without adequate security for data-in-process, a fairly serious problem could occur if the user's device is stolen and the thief is able to somehow substitute his biometric data to successfully authenticate fraudulent transactions using the legitimate owner's accounts.

As the designation Match-on-Host implies, the match and many other biometric processes are performed by host resources, and the processing itself can be made sufficiently secure for most applications using a TEE. By contrast, and also as its designation implies, the next-generation Match-in-Sensor solution performs the match and all other biometric processes entirely within the sensor System-on-Chip. With all processing occurring securely within the Match-in-Sensor SoC, there is never any need to make any biometric data available to the host operating system; therefore, there is no dependency on the host's TEE for privacy or security.

Total isolation from the host for processing biometric data means that even if the host is completely compromised by a successful attack of any type or origin, including one that affects the TEE, it is not possible to force the Match-in-Sensor solution to generate a false positive result, replay an old result, or in any other way alter or manipulate the match result. For this reason, Match-in-Sensor provides the best possible security for data-in-process because every process is performed entirely within the Synaptics proprietary SoC.

Securing Internal Commands

Communications among the various subsystems and resources contained within every device can also create potential vulnerabilities. These communications normally take the form of commands or instructions sent to an application programming interface (API). For biometric authentication, such communications can range from a simple request/reply with the Match-in-Sensor SoC to a more involved sequence of exchanges needed for Match-on-Host to read the scanner, access the template, compare the two, and reply with a positive or negative match result. During all of these exchanges, SentryPoint encrypts all requests and replies between the host processes and the biometric sensor IC(s) using Transport Layer Security (TLS). TLS is a cryptographic protocol that prevents an attacker from sending sensitive commands to the sensor, bypassing the driver and accessing the data on the wire to or from the sensor.

Securing Data-in-Flight

Whenever host resources are used to perform any of the requisite biometric functions, the biometric template data must be transferred to the host from the biometric sensor, as well as to/from the host from/to the memory where it is stored. Because these exchanges require command and control communications between processes during the data transfer, these commands are also in-flight and, therefore, must be secured (see *Securing Internal Commands,* in the left sidebar).

Data-in-flight creates the greatest vulnerability to potential exploits from malware infecting the host.

For example, malware could be designed to initiate and complete fraudulent online transactions that require user authentication by interfering with the match request/reply processing to produce a false positive match. Even worse is that these transactions are likely also designed to operate entirely in the background, leaving the user completely unaware there is a problem—until, that is, the bank calls or the statement arrives in the mail.

Securing data-in-flight is critical to preventing any tampering that would undermine the integrity of legitimate transactions, or be used to create fraudulent ones. With the next-generation Match-in-Sensor solutions, the only place biometric data is stored and processed is within the SoC, eliminating the need to put biometric data in-flight, and thereby eliminating this vulnerability. Match-in-Sensor also minimizes the need for commands by requiring only two exchanges with the host via the Synaptics API: once to enroll user's fingerprint in the template database; and as needed to authenticate the user with a match, requiring a simple "Yes/No" reply (shown in Figure 1). Because both the requests and replies are encrypted, they are incorruptible.

For Match-on-Host solutions, the techniques in the Synaptics SentryPoint security suite for making biometric data-in-flight secure are similar to the ones used to protect data-at-rest: strong 256-bit encryption with robust key management. There is one obvious difference, however: The need to use a secure communications protocol to access the biometric template, for which SentryPoint utilizes Transport Layer Security (TLS) that has been proven in numerous applications to ensure the validity and integrity of data being transferred.

For biometric forms of authentication that require even minimal processing in the host, this use of strong encryption and robust key management fully protects all commands- and data-in-flight. The resulting level of security is, therefore, established by the host's Trusted Execution Environment (TEE), which is normally made quite secure by most equipment manufacturers.

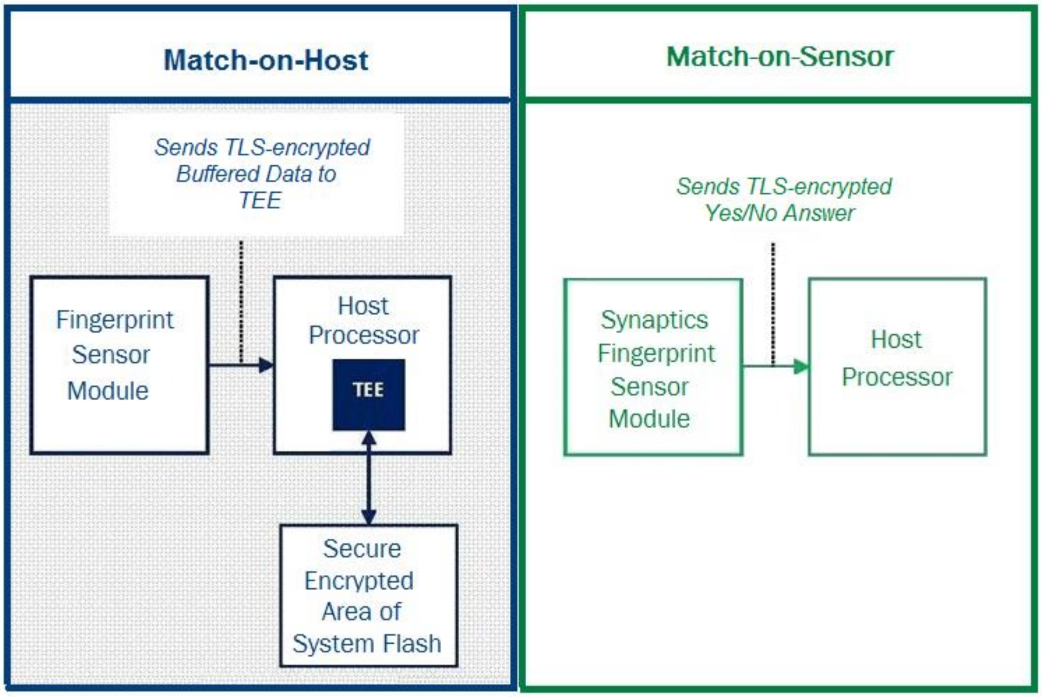
Match-on-Host
Sends TLS-encrypted Buffered Data to TEE
Fingerprint Sensor Module
Host Processor
TEE
Secure Encrypted Area of System Flash
Match-on-Sensor
Sends TLS-encrypted Yes/No Answer
Synaptics Fingerprint Sensor Module
Host Processor

Figure 1. Match-on-Host and Match-in-Sensor

With no data-in-flight ever, and all data-at-rest or in-process remaining entirely within the secure SoC module, the next-generation Match-in-Sensor architecture affords the best possible biometric security available today.

Conclusion

The many advantages of biometric authentication make it an increasingly common and competitive feature on smartphones, tablets and PCs. But the very private nature of biometric data and its decisive role in user authentication also make it critically important to protect it, in all of its states, within the device.

The Synaptics SentryPoint security suite protects biometric data while at rest, when in process and during flight using a variety of robust and proven techniques that give equipment manufacturers a wide range of options in device designs. These options involve making tradeoffs among cost, ease of implementation, level of security provided and other goals, and Synaptics engineers regularly consult with the device manufacturer design teams to help make the optimal set of choices.

For designs requiring the highest level of biometric sensing privacy and security available today, Synaptics offers the next-generation Match-in-Sensor architecture. Match-in-Sensor solutions:

- Protect biometric data at-rest with virtually impenetrable layers of security,
- Secure biometric data in-process by performing all tasks within the System-on-Chip, which is inherently more secure than any host-based Trusted Execution Environment, and
- Completely eliminate the need to ever put biometric data in-flight, which is when it becomes the most vulnerable.

More information about Match-in-Sensor solutions is available in a white paper titled *Fingerprint Sensing: The Next Generation* (PN: 507-000178-01). For more information about the SentryPoint security suite and the Match-in-Sensor and Match-on-Host solutions, visit Synaptics on the Web at www.synaptics.com.

About Synaptics

Synaptics is the pioneer and leader of the human interface revolution, bringing innovative and intuitive user experiences to intelligent devices. Synaptics' broad portfolio of touch, display, and biometrics products is built on the company's rich R&D and supply chain capabilities. With solutions designed for mobile, PC and automotive industries, Synaptics combines ease of use, functionality and aesthetics to enable products that help make our digital lives more productive, secure and enjoyable. (NASDAQ: SYNA) www.synaptics.com.

Copyright

Trademarks

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.