Intel® Hardware-based Security Technologies Bring Differentiation to Biometrics Recognition Applications
Part 1
Contents

Why Biometric Recognition is Better ................................................................. 3
How Biometric Recognition Works .................................................................... 4
The Attack Model ................................................................................................. 5
How Intel® Hardware-based Security Technologies Improve the Security of Biometrics Recognition ........................................................................................................... 6

1. Trusted Execution Environment with Intel® Software Guard Extensions .......... 6
   1.1 What is TEE? ........................................................................................................ 6
   1.2 Intel® Software Guard Extensions Technology Overview ................................. 7
   1.3 How to Harden Biometric Recognition Function by Intel® Software Guard Extensions Technology? ........................................................................................................... 9

2. Memory Protection Scheme with Virtual Machine Extensions ......................... 10
   2.1 The Weakness of the Legacy Software-Based Memory Protection .................. 11
   2.2 Memory Protection Based on Virtual Machine Extensions .............................. 11

3. Multiple Factor Authentication with Intel® Identity Protection Technology with One-Time Password ................................................................. 12

Link to Part 2 ........................................................................................................ 13
References .............................................................................................................. 13
Why Biometric Recognition is Better

The security model of “Username/Password” has been used as a user’s identity certificate for years. When people need to prove that they are authorized users of a service (the usual process is to log in to a computer or an online service, such as social media, or online banking), they input their username and password. The disadvantages of this security model are obvious for a number of reasons, including:

1. Simple passwords such as “123456” or “hello” can be cracked by a brute-force attack or a dictionary attack.
2. A complicated password is hard to remember.
3. Many people might use the same password across multiple sites.
4. If a person forgets the password, after providing some other identification, he or she can reset it.

To improve the strength of passwords and the user experience, more and more service providers are beginning to use biometric identification technology as the password. With this technology, people don’t need to remember their passwords. Instead their voice, face, fingerprint, or iris is used as the identifying factor. Biometric identification factors are somewhat different from the traditional username/password security model factors:

- Biometrics can be used to derive a long and complicated password, which offers greater security to withstand a brute-force attack.
- Biometrics require more security protection to a biometric recognition application developer, because biological information is part of the human body and cannot be changed easily. If biometric information is stolen, it is hard for a user to revoke his or her biometric password. An attacker can duplicate a fake human part by using the stolen biometrics and use it to pass the biometric check on other user registered accounts in future.
- Some biological characteristics such as face and voice have a high false acceptance rate. So a biometrics recognition system usually uses multi-biometric factor authentication to improve the recognition accuracy.
- Some biometrics characteristics can be duplicated, like a recorded voice, a printed photo of a face, or a gelatin finger from a fingerprint. It is important to add a vitality detection module into the biometric recognition system to identify whether the biometrics
information is from a live person or from a replicate object.

**How Biometric Recognition Works**

The basic flow of a biometric recognition application has five steps:

1. Biometric information is collected by the sensor, which is connected through the I/O port.
2. The output data format and speed is controlled by the specific device driver. Data is processed via the driver to meet the OS requirement at Ring-0 level and then sent to the biometric verification app, which is running at Ring-3.
3. Once the app gets the data, it does some preprocessing work and extracts the feature points from the data.
4. Next, the extracted feature points are sent to the pattern matcher and compared with registered biometric patterns in the database.
5. Once the pattern matches with one of the registered patterns, the matcher sends the MATCH message, and the UI procedure will display that the user is logged in correctly and show the corresponding premier content to the user.

![Diagram of biometric recognition program flow](image)

*Figure 2. The flow chart of a biometric recognition program.*
The Attack Model

In a biometric-based authentication system, the most valuable data to an attacker is the user’s biometric pattern. This pattern could be the raw data from a sensor, the extracted feature point set in memory, or the registered biological pattern stored in the database.

In general, if the biometric recognition application is designed without proper security protection, the attacker could retrieve the raw data or feature point set from memory via runtime attack by using a rootkit or malware. The attacker could also launch an offline attack to get the registered biological pattern if the registration template is stored at the local storage of the device. Moreover, the attacker could sniff the data stream from a data bus between the processor and the sensor or by using a camera or microphone near the user to get some biometric data like face pictures or voice samples for a further replay attack.

From the perspective of a biometrics recognition service developer, the design philosophy of the application should provide end-to-end protection to keep a user’s privacy safe. This includes:

- Provide a trusted running environment to keep the integrity of the application code segment.
- Protect the memory region, which contains the biometric pattern, from access by other applications.
- Keep the sensitive data with strong encryption when it is in memory/local storage (or exchange the secret data between other applications or the network server).

Figure 3. Possible attacks on a biometrics recognition application.
How Intel® Hardware-based Security Technologies Improve the Security of Biometrics Recognition

Intel's platform offers various hardware-based security technologies to satisfy the security requirements for biometric verification applications.

1. Trusted Execution Environment with Intel® Software Guard Extensions

Biometric recognition technology is being used more and more widely because of its security. Because the technology is based on the unique characteristics—face, voice, fingerprint, iris—of each dedicated person, a person's identity is hard to steal. Biometric recognition technology takes the place of traditional password authentication and offers a good user experience.

However, with the wide use of biometric recognition technology in various consumer devices, the diversity and openness of the platform has raised some potential security threats. One threat that developers need to carefully consider is how to secure the operation of a biometric identification function on a variety of terminal devices. In particular they need to consider:

- How to securely run the biometric sampling/modeling/matching algorithm on the terminal device
- How to securely store biometric data template on the terminal device
- How to establish a secure channel link between the terminal device and the cloud database of biological characteristics, to complete the cloud authentication and other operations

Developers can rely on Trusted Execution Environment (TEE) technology to build an effective hardened solution.

1.1 What is TEE?

TEE is an isolated, trusted execution environment isolated from the Rich Execution Environment (REE).

According to the Global Platform TEE System Architecture specification [1], at the highest level, a
TEE is an environment where the following are true:

- Any code executing inside the TEE is trusted in authenticity and integrity.
- The other assets are also protected in confidentiality.
  - The TEE shall resist all known remote and software attacks, and a set of external hardware attacks.
- Both assets and code are protected from unauthorized tracing and control through debug and test features.

1.2 Intel® Software Guard Extensions Technology Overview

Intel® Software Guard Extensions (Intel® SGX) enables SW developers to develop and deploy secure applications on PC open platforms. It is a set of new instructions and memory access changes added to Intel® architecture.

Intel® SGX operates by allocating hardware-protected memory where code and data reside. The protected memory area is called an enclave. Data within the enclave memory can only be accessed by the code that also resides within the enclave memory space. Enclave code can be invoked via special instructions. An enclave can be built and loaded as a Windows® DLL.

One Intel® SGX technology-enabled application is built as an untrusted part and a trusted part following the Intel® SGX design framework [2]. When the application is running, it calls Intel® SGX special instructions to create an enclave, which is placed in trusted memory. When the trusted function is called, the code is running inside the enclave, and the relevant data can be seen in clear text only inside the enclave. Any external access to this data is denied. After the trusted function returns, the enclave data remains in trusted memory.
The objective of this Intel® technology is to enable a high-level protection of secrets. The application gains the ability to defend its own secrets thanks to Intel® SGX technology. Sensitive data is protected within applications. The attack surface, or TCB (Trusted Computing Base), is minimized as application self and processor. Even the malware that subverts OS/VMM, BIOS, drivers, etc. cannot steal the application secrets.
1.3 How to Harden Biometric Recognition Function by Intel® Software Guard Extensions Technology?

Before we discuss the security solution proposal for biometric recognition, we should address which factors should be protected during the process:

- The user’s private biometric characteristics data should be handled carefully in application, at rest, and in flight.
- The biometric operation algorithm, including sampling, modeling, and matching, should be protected against viruses and malware. The output result data should not be tampered with.

We proposed the architecture shown in Figure 7.

![Figure 7. Hardened biometric recognition function by Intel® Software Guard Extensions.](image)

The biometric sampling/modeling/matching algorithm is hosted inside the Intel® SGX enclave, the trusted part of the client, and is responsible for operating on the biometric characteristics data. Its runtime confidentiality and integrity is guaranteed. This type of algorithm is normally software implementation. Normal software implementation may be tampered with at runtime by viruses and malware. But in this architecture, at runtime, the protected portion is loaded into an enclave where its code and data is measured. Once the application’s code and data is loaded into an enclave, it is protected against all external software access. So the biometric operation algorithm can be trusted. Beyond the security properties, the enclave environment offers scalability and performance associated with execution on the main CPU of an open platform. So it is helpful for the performance sensitive scenario, especially the biometric recognition function.

Intel® SGX technology provides a function to encrypt and integrity-protect enclave secrets to store them outside the enclave, such as on disk, and the application can reuse this data later. Data can be sealed against an enclave using a hardware-derived Seal Key. The Seal Key is unique to the CPU and the specific enclave environment. Combined with other services, like Monotonic Counter or Trusted Time, which are provided by the Intel® SGX Platform Software, the solution can be used to protect against various attack techniques. The Monotonic Counter can be used to implement...
replay-protected policy, and the Trusted Time can be used to enforce a time-based policy. Both of them are in a form of Sealed Data. The enclave is responsible for performing the encryption with an algorithm of its choice; in other words, the developer can choose any encryption framework according to their system security requirement. So we can keep the user’s privacy biometric characteristics data to be handled only within the enclave and make sure that its raw data cannot be exposed to the untrusted part out of the enclave.

Sometimes the client biometric recognition function needs to connect to the remote back-end server to do authentication in the cloud database instead of locally. Using Intel® SGX attestation capabilities, the client authentication module authenticates the client platform and user’s biometric characteristics data with the remote server. Attestation is the process of demonstrating that a piece of software has been properly instantiated on the platform. In Intel® SGX it is the mechanism by which another party can gain confidence that the correct software is securely running within an enclave on an enabled platform.

First, this module generates a verifiable report of the client’s identity that is bound to the platform by the CPU [3]. The report also includes information about the user running the biometric recognition session. The server verifies the report to ensure that it is communicating with a device that is enabled with Intel® SGX. The client and server engage in a one-time provisioning protocol that results in application secrets being securely sealed to the client platform, using Intel® SGX sealing capabilities.

These secrets, which can only be unsealed by the application that sealed it, are used to establish secure sessions with the server in the future, without the need for constantly proving the identity of the client platform. Such secrets can be salt, encryption key, policy, certificate, etc. After that, the biometric characteristics data and authentication result can be sent through the secure communication channel between the client and server.

2. Memory Protection Scheme with Virtual Machine Extensions

Dynamic data attack is one of the most commonly known attack methodologies. Rootkit and malware can use this technique to hook a specified function and dump/modify data in the memory at runtime. In the case of biometrics recognition, malicious code can get the biometric data captured from the sensor and registered user biometric template from memory.
2.1 The Weakness of the Legacy Software-Based Memory Protection

Traditional software-based memory protection mechanisms are not reliable enough. Both the protection code and malicious code are running at the same privilege (ring-0 or ring-3). So malware can compromise the protection code easily to disable the protection.

![Diagram showing attacks on memory protection modules](attachment:diagram.png)

Figure 8. Attacks can compromise the protection module and access the sensitive data buffer.

2.2 Memory Protection Based on Virtual Machine Extensions

Virtual Machine Extensions (VMX) is a set of instructions that support virtualization of processor hardware [4]. Its basic working logic is:

- Ignore the basic CPU operation like load/store, branch and ALU operations
- Monitor (trap) the privileged instructions such as MMU manipulation, I/O instructions or update the TLB
- If a privilege instruction is executed, break the execution and set CPU into VMX root mode for further processing

The following diagram shows the relationship between the hardware/OS/application with VMM mode enable/disable.
By utilizing the hardware-based trap function of VMX, a hardware virtualization-based memory protection mechanism can protect memory in a safer and faster way [5]. The basic idea is to insert a VMM-based memory monitor module between the OS and hardware. When loading the application, build a memory map table for the trusted code region and data region. After building the table, whenever there is memory access, VMM can trap it, then compare the memory access instruction address (EIP) and memory address with the pre-built table. Then the memory protection module can identify whether this is a legal or illegal access and apply for the corresponding process.

3. Multiple Factor Authentication with Intel® Identity Protection Technology with One-Time Password

Identity theft is a growing global concern for individuals and businesses. Secure, but simple-to-use solutions are required as hackers devise new methods for obtaining usernames and passwords. Hackers never stop devising new ways to steal usernames and passwords. If you are a consumer or an everyday computer user, Intel® Identity Protection Technology (Intel® IPT) provides strong techniques for avoiding the threat of identity theft by giving you the opportunity to link your physical device to each Intel® IPT-enabled online account that you use.

Traditionally, two-factor authentication uses a one-time password (OTP) which combines something the user knows (a username and password) and something the user has (typically, a token or key fob that produces a six-digit number, valid only for a short period of time and available on demand).

In the case of Intel® IPT with OTP [6], a unique, one-time use, six-digit number is generated every 30 seconds from an embedded processor that is tamper-proof and operates in isolation from the OS. Because the credential is protected inside the chipset, it cannot be compromised by malware or removed from the device.
Figure 10. Intel® Identity Protection Technology with one-time password authentication working flow between client and server.

If your business is already using two-factor authentication, you are already familiar with the various issues around token usability and logistics. Intel® IPT with OTP is a built-in hardware token (with your security vendor of choice) that negates the need for a separate physical token, thus simplifying the two-factor VPN log-in process for a seamless experience with virtually no delays.

With Intel® IPT with OTP on Intel® processor-based devices, Intel provides a hardware root of trust, proof of a unique Intel processor-based device, to websites, financial institutions, and network services that it is NOT malware logging into an account. Intel® IPT with OTP enabled systems offer additional identity protection and transaction verification methods that can be utilized by multifactor authentication solutions.

**Link to Part 2**

**References**


Notices
Intel technologies’ features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. Check with your system manufacturer or retailer or learn more at intel.com.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest forecast, schedule, specifications and roadmaps.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting [www.intel.com/design/literature.htm](http://www.intel.com/design/literature.htm).

This sample source code is released under the Intel Sample Source Code License Agreement.

Intel, the Intel logo, Intel Atom, and Intel RealSense are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others
© 2015 Intel Corporation.