Apple T2 Security Chip

Security Overview

October 2018

Contents

Introduction

The Apple T2 Security Chip, our second-generation custom Mac silicon, brings industry-leading security to Mac. It features a Secure Enclave coprocessor, which provides the foundation for APFS encrypted storage, secure boot, and Touch ID on Mac. In addition to the security components, the T2 chip integrates several controllers found in other Mac systems—like the system management controller, image signal processor, audio controller, and SSD controller.

A dedicated AES hardware engine included in the T2 chip powers line-speed encrypted storage with FileVault. FileVault provides data-at-rest protection for Mac.

The T2 chip is the hardware root of trust for secure boot. Secure boot ensures that the lowest levels of software aren't tampered with and that only trusted operating system software loads at startup.

On Mac computers with Touch ID and the T2 chip, the Secure Enclave also secures Touch ID. In addition, all Mac portables with the T2 chip have a hardware disconnect that ensures the microphone is disabled when the lid is closed.

The features of the Apple T2 Security Chip are made possible by the combination of silicon design, hardware, software, and services available only from Apple. These capabilities combine to provide unrivaled privacy and security features never before present on Mac.

Secure Enclave

The Secure Enclave is a coprocessor fabricated within the system on chip (SoC) of the Apple T2 Security Chip, built solely to provide dedicated security functions. It protects the necessary cryptographic keys for FileVault and secure boot, and is also responsible for processing fingerprint data from the Touch ID sensor (if present) and determining if there's a match.

The Secure Enclave on the T2 chip uses encrypted memory and includes a hardware random number generator. It maintains the integrity of its security functions even if the macOS kernel has been compromised, and its limited function is a virtue: Security is enhanced by the fact that the hardware is limited to specific operations.

All Apple FIPS 140-2 Conformance Validation Certificates are on the CMVP vendor page. For information on the status of FIPS certification of the Apple T2 Security Chip, go to: https://support.apple.com/HT208675.

Storage Encryption

APFS encrypted storage

The Apple T2 Security Chip provides a dedicated AES crypto engine built into the DMA path between the flash storage and main system memory (see Figure 1), making internal volume encryption using FileVault with AES-XTS highly efficient.

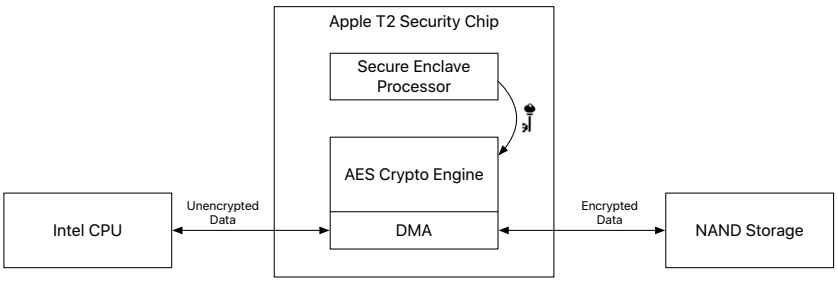

Figure 1: AES Crypto Engine

The Mac unique ID (UID) and a device group ID (GID) are AES 256-bit keys fused (UID) or compiled (GID) into the Secure Enclave during manufacturing. No software or firmware can read the keys directly. The keys can be used only by the AES engine dedicated to the Secure Enclave. This dedicated AES engine makes available only the results of encryption or decryption operations it performs. The UIDs and GIDs aren't available via JTAG or other debugging interfaces.

Because the UID is unique to each device and is generated wholly within the Secure Enclave rather than in a manufacturing system outside of the device, the UID key isn't available for access or storage by Apple or any Apple suppliers. Software running on the Secure Enclave takes advantage of the UID to protect device-specific secrets such as Touch ID data, FileVault class keys, and the Keychain.

The UID allows data to be cryptographically tied to a particular device. For example, the key hierarchy protecting the file system includes the UID, so if internal storage media are physically moved from one device to another, the files they contain are inaccessible. The UID isn't related to any other identifier on the device. This architecture forms the basis for secure internal volume encryption.

Internal volume encryption and FileVault

In Mac OS X 10.3 or later, Mac computers provide FileVault, built-in encryption capability to secure all data at rest. FileVault uses the AES-XTS data encryption algorithm to protect full volumes on internal and removable storage devices.

On Mac computers with the Apple T2 Security Chip, internal volume encryption leverages the hardware security capabilities of the chip. After a user enables FileVault on a Mac, their credentials are required during the boot process.

External media

Encryption of external media doesn't utilize the security capabilities of the Apple T2 Security Chip, and its encryption is performed in the same manner as Mac computers without the T2 chip.

Without valid login credentials or a cryptographic recovery key, the internal APFS volume remains encrypted and is protected from unauthorized access even if the physical storage device is removed and connected to another computer. Internal volume encryption on a Mac with the T2 chip is implemented by constructing and managing a hierarchy of keys (see Figure 2), and builds on the hardware encryption technologies built into the chip. This hierarchy of keys is designed to simultaneously achieve four goals:

- Require the user's password for decryption.
- Protect the system from a brute-force attack directly against storage media removed from Mac.
- Provide a swift and secure method for wiping content via deletion of necessary cryptographic material.
- Enable users to change their password (and in turn the cryptographic keys used to protect their files) without requiring re-encryption of the entire volume.

On Mac systems with the T2 chip, all FileVault key handling occurs in the Secure Enclave; encryption keys are never directly exposed to the (Intel) application processor.

All APFS volumes are created with a volume key by default. Volume and metadata contents are encrypted with this volume key, which is wrapped with the class key. The class key is protected by a combination of the user's password and the hardware UID when FileVault is enabled. This protection is the default on Mac computers with the T2 chip.

If FileVault isn't enabled on a Mac with the T2 chip during the initial Setup Assistant process, the volume is still encrypted, but the volume key is protected only by the hardware UID in the Secure Enclave. If FileVault is enabled later—a process that is immediate since the data was already encrypted—an anti-replay mechanism prevents the old key (based on hardware UID only) from being used to decrypt the volume. The volume is then protected by a combination of the user password with the hardware UID as previously described.

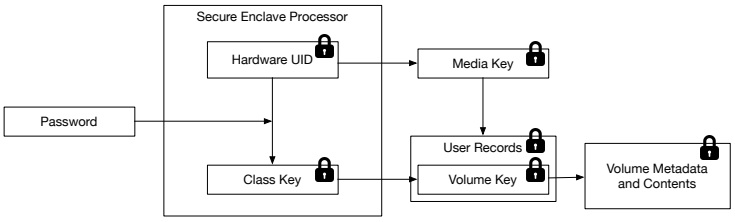

Figure 2: FileVault key hierarchy

When deleting a volume, its volume key is securely deleted by Secure Enclave. This prevents future access with this key even by the Secure Enclave. In addition, all volume keys are wrapped with a media key. The media key doesn't provide additional confidentiality of data, but instead is designed to enable swift and secure deletion of data because without it, decryption is impossible.

The media key is located in effaceable storage and designed to be quickly erased on demand; for example, via remote wipe using Find My Mac or when enrolled in a mobile device management (MDM) solution. Effaceable storage accesses the underlying storage technology (for example, NAND) to directly address and erase a small number of blocks at a very low level. Erasing the media key in this manner renders the volume cryptographically inaccessible.

Delays between password attempts

Attempts	Delay Enforced
1–14	none
15–17	1 minute
18–20	5 minutes
21–26	15 minutes
27–30	1 hour

To further discourage brute-force attacks, there are escalating time delays after the entry of an invalid password at the Login Window or via Target Disk Mode. The delays are enforced by the Secure Enclave coprocessor on the T2 chip. If Mac is restarted during a timed delay, the delay is still enforced, with the timer starting over for the current period.

To prevent malware from causing permanent data loss, no wipe occurs when limits are reached while booted into macOS. Instead, 10 more attempts are available after booting into macOS Recovery. If those 10 attempts are exhausted, then a further 90 attempts are possible using a combination of each type of enabled FileVault recovery mechanism (30 each for iCloud recovery, FileVault recovery key, and institutional key). Once all those attempts are exhausted, data on the volume can't be recovered.

Secure boot

For Mac computers with the Apple T2 Security Chip, each step of the startup process contains components that are cryptographically signed by Apple to verify integrity (see Figure 3). The boot process proceeds only after verifying the integrity of the software at every step, which creates a chain of trust rooted in hardware. This includes the UEFI firmware, bootloaders, kernel, and kernel extensions necessary for boot. This secure boot chain helps ensure that the lowest-level software isn't tampered with, so the Mac computer will be in a known trustworthy state when it's booted.

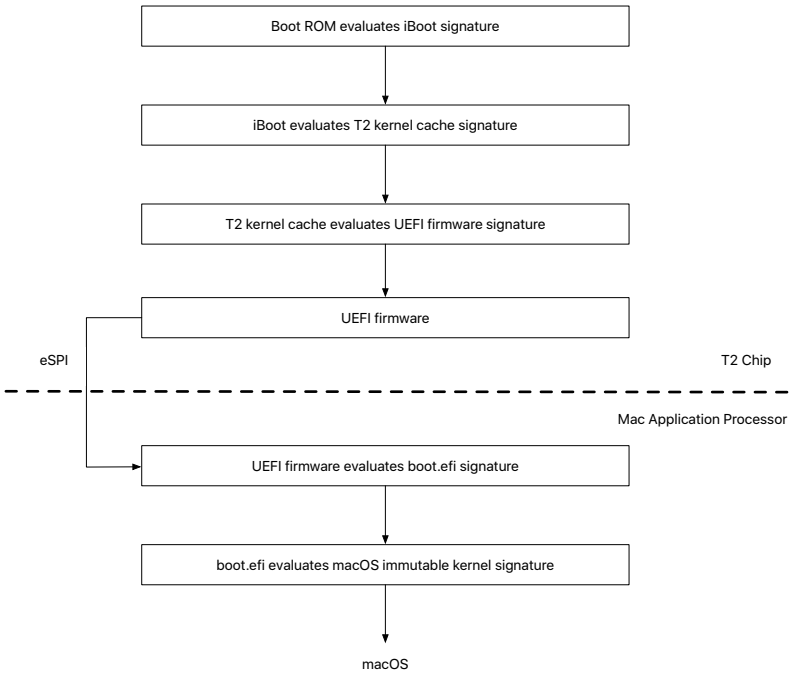

Figure 3: macOS secure boot chain

When a Mac computer with the T2 chip is turned on, the chip executes code from read-only memory known as the Boot ROM. This immutable code, referred to as the hardware root of trust, is laid down during chip fabrication and is audited for vulnerabilities and implicitly trusted. The Boot ROM code contains the Apple Root CA public key, which is used to verify that the iBoot bootloader is signed by Apple's private key before allowing it to load. This is the first step in the chain of trust. iBoot verifies the kernel and kernel extension code on the T2 chip, which subsequently verifies the Intel UEFI firmware. The UEFI firmware and the associated signature are initially available only to the T2 chip.

After verification, the UEFI firmware image is mapped into a portion of the T2 chip memory and this memory is made available to the (Intel) application processor via the enhanced Serial Peripheral Interface (eSPI). When the application processor first boots, it fetches the UEFI firmware via eSPI from the integrity-checked, memory-mapped copy of the firmware located on the T2 chip.

The evaluation of the chain of trust continues on the application processor, with the UEFI firmware evaluating the signature for boot.efi, which is the macOS bootloader. The Intel-resident macOS secure boot signatures are stored in the same Image4 format used for iOS and T2 chip secure boot, and the code that parses the Image4 files is the same hardened code from the current iOS secure boot implementation. Boot.efi in turn verifies the signature of a new file called *immutablekernel*. When secure boot is enabled, the immutablekernel represents the complete set of Apple kernel extensions required to boot macOS. The secure boot policy terminates at the handoff to the immutablekernel, and after that, macOS security policies (such as System Integrity Protection and signed kernel extensions) take effect.

Any errors or failures in this process result in Mac entering macOS Recovery mode, Apple T2 Security Chip recovery mode, or Apple T2 Security Chip DFU mode.

Alternate boot modes

Beyond booting macOS, there are a variety of alternate boot behaviors on Mac, all of which are also protected by secure boot. These include Recovery mode, Diagnostics mode, and Internet Recovery mode. All modes proceed after successful verification of the integrity of the critical system files used for the boot mode—whether stored locally or downloaded from the Internet. In addition, while the connection to the OS Recovery Server is done via HTTP, the complete downloaded contents are still locally checked for cryptographic integrity.

Other boot-related features, such as Target Disk Mode, the Startup Manager, and the firmware password user interface, are all implemented as UEFI applications built into the main UEFI firmware. As such, they are verified as part of the T2 chip verification of the UEFI firmware, and don't require additional verification.

Microsoft Windows boot

By default, Mac computers supporting secure boot only trust content signed by Apple. However, in order to improve the security of Boot Camp installations, support for secure booting Windows is also provided. The UEFI firmware includes a copy of the Microsoft Windows Production CA 2011 certificate used to authenticate Microsoft bootloaders.

NOTE: There is currently no trust provided for the the Microsoft Corporation UEFI CA 2011, which would allow verification of code signed by Microsoft partners. This UEFI CA is commonly used to verify the authenticity of bootloaders for other operating systems such as Linux variants.

Support for secure boot of Windows isn't enabled by default; instead, it is enabled via Boot Camp Assistant (BCA). When a user runs BCA, Mac is reconfigured to trust Microsoft first-party signed code during boot. After BCA completes, if the system fails to pass the Apple first-party trust evaluation during secure boot, the UEFI firmware attempts to evaluate the trust of the object according to UEFI Secure Boot formatting. If this succeeds, it proceeds and boots Windows. If not, it enters macOS Recovery and informs the user of the trust evaluation failure.

Boot Recovery Assistant

In the event of a problem with secure boot or external boot, the UEFI firmware sets an error reason in an UEFI variable, and then boots into macOS Recovery. macOS Recovery then launches the Boot Recovery Assistant application, which tries to automatically correct the issue or inform the user of the issue and ask how they would like to proceed. Boot Recovery Assistant is also used to react to other forms of boot failure that might occur.

Startup Security Utility

Startup Security Utility is a replacement for Firmware Password Utility. On Mac computers with the Apple T2 Security Chip, this utility handles a larger set of security policy settings (see Figure 4). This utility is accessible by booting into macOS Recovery and selecting Startup Security Utility from the Utilities menu. The entirety of macOS Recovery, including Startup Security Utility, is cryptographically integrity-checked.

Secure boot policy

This policy is only shown in Startup Security Utility on computers with the T2 chip. The user is in control of the device's settings, and may choose to disable or downgrade the secure boot functionality.

Secure boot policy changes made from within this app only apply to the evaluation of the chain of trust being verified on the (Intel) application processor. Secure boot of T2 chip firmware is always in effect.

Figure 4: Startup Security Utility

Authentication in Recovery

Critical policy changes now require authentication, even in Recovery mode. This feature is available only on Mac computers containing the T2 chip or later. When Startup Security Utility is first opened, it prompts the user to enter an administrator password from the primary macOS installation associated with the currently booted macOS Recovery. If no administrator exists, one must be created before the policy can be changed. The chip requires that the Mac computer is currently booted into macOS Recovery and that an authentication with a Secure Enclave–backed credential has occurred before such a policy change can be made.

Security policy changes have two implicit requirements. macOS Recovery must be:

- Booted from an internal drive, because partitions on external devices don't have Secure Enclave–backed credentials bound to the internal system.
- On an APFS-based volume, because there is support only for storing the Authentication in Recovery credentials sent to the Secure Enclave on the "Preboot" APFS volume of a drive. HFS-formatted volumes can't use secure boot.

Secure boot policy can be configured in one of three ways:

- **Full Security:** Ensures that only the current macOS, or signed operating system software currently trusted by Apple, can boot the computer. This includes Windows (if enabled via Boot Camp Assistant). This setting prevents the installation of older copies of macOS (a key component of downgrade attacks) if those copies are not still being signed by Apple.
- **Medium Security:** Allows any signed operating system software ever trusted by Apple to boot the computer. This setting allows the installation of older copies of macOS even if they are *not* currently being signed by Apple. This method is only functional as long as the copy was previously signed by Apple and it hasn't been tampered with.
- **No Security:** Completely disables secure boot evaluation on the application processor and allows any operating system to boot the computer.

Full Security is the default configuration on a Mac with the T2 chip. When an operating system is being installed, the system communicates to an Apple Signing Server and requests a personalized signature that includes the ECID—a unique ID specific to the chip—as part of the signing request. The signature is unique and usable only by the operating system with that T2 chip installed. Therefore, when Full Security is configured, the T2 chip ensures the operating system is uniquely signed for each computer.

Full Security and external media

A copy of macOS on an external drive won't necessarily already be personalized for a Mac the first time it is booted. In this case, the first time a user attempts to boot from the external drive, Mac boots into Recovery, and Boot Recovery Assistant makes the signing request to Apple so it can obtain the necessary personalized signature. This is automatic, and looks like a longer boot process with a progress bar. Subsequent boots proceed normally.

External Boot policy

External Boot policy controls whether a Mac can be booted from external media. This policy is shown only on Mac computers with the T2 chip and is independent from the secure boot policy. Disabling secure boot doesn't change the default behavior of disallowing boot from external drives.

Touch ID

Using Touch ID on Mac is an easy way to use a fingerprint instead of a password for many common operations. With just the touch of a finger, the sensor quickly reads a fingerprint and automatically unlocks the device. Touch ID can authorize purchases from the iTunes Store, App Store, and Apple Books, as well as with Apple Pay.

Touch ID doesn't store any fingerprint images, instead it relies only on a mathematical representation of the fingerprint. This representation is encrypted, stored on the device, and protected with a key available only to the Secure Enclave. The fingerprint data is used only by the Secure Enclave to verify a match with the enrolled information. It can't be accessed by macOS or by any apps running on it. It's never stored on Apple servers, it's never backed up to iCloud or anywhere else, and it can't be used to match against other fingerprint databases.

Every fingerprint is unique, so it's rare that even a small section of two separate fingerprints are alike enough to register as a match for Touch ID. The probability of this happening is 1 in 50,000 with a single enrolled finger. And Touch ID allows only five unsuccessful fingerprint match attempts before requiring a password.

A password is required to start using Touch ID and a password is always required for viewing or changing password settings. A password is also required if Mac is in the following states:

- The device has just been turned on or restarted.
- The device hasn't been unlocked for more than 48 hours.
- The password hasn't been used to unlock the device in the last 156 hours (six and a half days) and a biometric hasn't unlocked the device in the last 4 hours.
- The device has received a remote lock command.
- After five unsuccessful attempts to match a fingerprint.

Hardware microphone disconnect

All Mac portables with the Apple T2 Security Chip feature a hardware disconnect that ensures that the microphone is disabled whenever the lid is closed. This disconnect is implemented in hardware alone, and therefore prevents any software, even with root or kernel privileges in macOS, and even the software on the T2 chip, from engaging the microphone when the lid is closed. (The camera is not disconnected in hardware because its field of view is completely obstructed with the lid closed.)

Conclusion

A commitment to security

The Apple T2 Security Chip provides a robust foundation for encrypted storage, secure boot, and Touch ID. These features are based on dedicated security hardware and the Secure Enclave coprocessor, which is included on the T2 chip. The resulting system is a Mac that can base the cryptographic protections of stored data in dedicated hardware and utilize a hardware root of trust to ensure secure boot. And on Mac systems with Touch ID, users can conveniently unlock their Mac with their finger. Combining the T2 chip with a hardware disconnect to ensure the microphone is disabled when the lid is closed results in a level of privacy and security protections never before seen on Mac.

To learn more about reporting issues to Apple and subscribing to security notifications, go to: https://www.apple.com/support/security.

Glossary

AES	Advanced Encryption Standard.
AES crypto engine	A dedicated hardware component that implements AES.
AES-XTS	A mode of AES defined in IEEE 1619-2007 meant to work for encrypting storage media.
APFS	Apple File System.
Boot Camp	Boot Camp supports the installation of Microsoft Windows on a Mac.
Boot ROM	The very first code executed by a device's processor when it first boots. As an integral part of the processor, it can't be altered by either Apple or an attacker.
DMA	Direct memory access enables hardware subsystems to access main memory.
Effaceable Storage	A dedicated area of NAND storage, used to store cryptographic keys, that can be addressed directly and wiped securely. While it doesn't provide protection if an attacker has physical possession of a device, keys held in Effaceable Storage can be used as part of a key hierarchy to facilitate fast wipe and forward security.
eSPI	Enhanced Serial Peripheral Interface bus for synchronous serial communication.
File system key	The key that encrypts each file's metadata, including its class key. This is kept in Effaceable Storage to facilitate fast wipe, rather than confidentiality.
Group ID (GID)	Like the UID, but common to every processor in a class.
iBoot	Code that's loaded by LLB, and in turn loads XNU, as part of the secure boot chain.
Joint Test Action Group (JTAG)	Standard hardware debugging tool used by programmers and circuit developers.
Mobile device management (MDM)	A service that lets you remotely manage enrolled devices. Once a device is enrolled, you can use the MDM service over the network to configure settings and perform other tasks on the device without user interaction.
NAND	Nonvolatile flash memory.
SSD controller	Hardware subsystem that manages the storage media (solid-state drive).
T2 DFU mode	Device Firmware Upgrade mode for the Apple T2 Security Chip.
UEFI firmware	Unified Extensible Firmware Interface, a replacement technology for BIOS to connect firmware to the operating system of a computer.
Unique ID (UID)	A 256-bit AES key that's burned into each processor at manufacture. It can't be read by firmware or software, and is used only by the T2 chip's hardware AES engine. To obtain the actual key, an attacker would have to mount a highly sophisticated and expensive physical attack against the processor's silicon. The UID isn't related to any other identifier on the device including, but not limited to, the UDID.