How does the security chip on smartphones work?

On each smartphone, there is a security chip that protects the user's device. For example, Google's Pixel 3 is a Titan M chip, on Apple's iPhone is Secure Enclave, and Samsung's Galaxy smartphone and some Android devices are ARM's TrustZone technology.

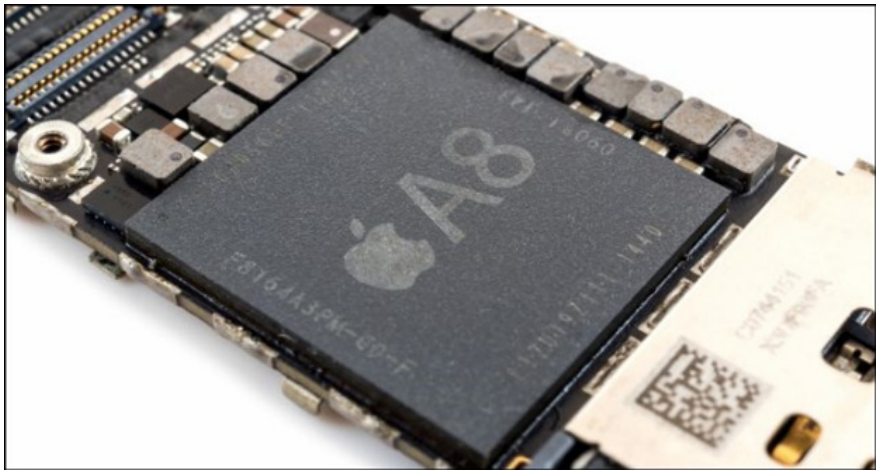
On each smartphone, there is a security chip that protects the user's device. For example, Google's Pixel 3 is a Titan M chip, on Apple's iPhone is Secure Enclave, and Samsung's Galaxy smartphone and some Android devices are ARM's TrustZone technology. So how do these security chips work? Follow the article below for answers.

Basic information

Basically, these security chips are microcomputer computers that have microprocessors, native memory and run their own tiny operating systems. They work independently of other devices in the phone.

The normal operating system as well as the applications that operate on it in the phone will not be able to access this secure area. Therefore, this complete chip is isolated and not compromised, they can do many useful things.

The behavior of each security chip is different. Titan M on Google's new Pixel is a physical chip that is separate from the CPU of the machine.



Secure Enclave is directly integrated into Apple's A-series SoC.

ARM's Secure Enclave and TrustZone are a stand-alone processor integrated directly into the device's main SoC. Although they are not a separate chip, they still have a processor and a separate memory area. Or it can be said, they are like a chip inside the main chip.

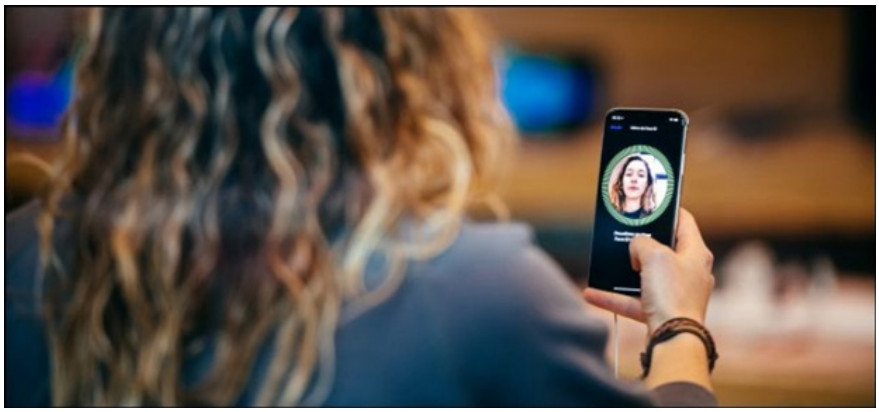
Data on the phone is encrypted on memory and unlock code is stored in the secure area. When the user unlocks the phone, the processor inside the security area will authenticate the user identity. Then, the unlock code will be used to decrypt the data in memory.

Security chip will prevent bad guys from entering PIN or password many times. Even if the bad guys have logged in to the phone, the security chip will also not allow them to access the device's security key.

1. What is Apple's Secure Enclave and how does it protect iPhone and Mac?
2. Titan M chip makes Google Pixel 3 more difficult to hack, protect bootloader

Why does the phone need a secure processor?

The security chip will protect the critical data of users such as encryption keys and payment information. This helps keep users' security information secure even if the device is tampered with. Even if another modified operating system is installed instead of the device's operating system, the security chip still does not allow them to access your device.



Secure stored user billing information ensures that no malware running on your device can access them.

On Titan M chips, Google also integrated new features to ensure the attacker could not downgrade the operating system or replace the Titan M. firmware.

Even crypto chips can resist Specter-style attacks that allow the application to read the memory that does not belong to it because the memory chip is completely separate from the system's main memory.

Security chips work silently to protect the phone and data for users. Most users are unaware of this hardware detail and they probably don't need to know because manufacturers will do everything to enhance the security of modern smartphones and protect them from attacks. could happen.

See more:

1. If you don't want to be a victim of Ransomware, read this article
2. Cold boot, an attack technique 10 years ago can crack the encryption of most PCs today
3. Super secure SIM card, only connecting data via Tor anonymity network helps protect information for users