|  |  |
| --- | --- |
| **Device integrity**  Device integrity features protect the mobile device from any changes to the operating system. With companies using mobile devices for essential communication and core productivity tasks, keeping the OS secure is essential. Without device integrity, very few security properties can be assured. Android adopts several measures to guarantee device integrity at all times. Verified Boot [Verified Boot](http://source.android.com/security/verifiedboot/index.html)​ mitigates attacks against devices by providing a boot process that verifies system software using a hardware root of trust. This makes it more difficult for software attacks to result in a persistent OS compromise, and provides users with a safe state at boot time.  Each Verified Boot stage is cryptographically signed. Each phase of the boot process verifies the integrity of the subsequent phase, prior to executing that code. As of Android 7.0, full boot of a compatible device with a locked bootloader proceeds only if the operating system satisfies integrity checks.  As of Android 8.1, device implementations with more than 1GB of RAM must support Verified Boot for device integrity. Verification algorithms used must be as strong as current recommendations from NIST for hashing algorithms (SHA-256) and public key sizes (RSA-2048).  The Verified Boot state is used as an input in the process to derive disk encryption keys. If the Verified Boot state changes (e.g. the user unlocks the bootloader), then the secure hardware prevents access to data used to derive disk encryption keys.  Verified Boot on compatible devices running Android 8.0 and higher enables rollback protection. This means that a kernel compromise (or physical attack) cannot put an older, more vulnerable, version of the OS on your system and boot it. Additionally, rollback protection state is also stored in tamper-evident storage.  Enterprises can check the state of Verified Boot using​ [KeyStore key attestation](https://developer.android.com/training/articles/security-key-attestation.html)​[.](https://developer.android.com/training/articles/security-key-attestation.html) This retrieves a statement signed by the secure hardware attesting to many attributes of Verified Boot along with other information about the state of the device. KeyStore key attestation is required in devices shipped with Android 8.0 onwards.    Find out more about Verified Boot ​[here.](https://source.android.com/security/verifiedboot/)​ | **Integrità del dispositivo** Le funzionalità di integrità proteggono il dispositivo mobile da qualsiasi modifica al sistema operativo. Poiché le aziende utilizzano i dispositivi mobili per la comunicazione essenziale e le attività essenziali di produttività, è fondamentale mantenere il sistema operativo sicuro. Senza l’integrità del dispositivo, è possibile assicurare pochissime proprietà di sicurezza. Android adotta diverse misure per garantire l’integrità del dispositivo in qualsiasi momento. Avvio verificato [L’Avvio verificato](http://source.android.com/security/verifiedboot/index.html) mitiga gli attacchi contro i dispositivi fornendo un processo di avvio che verifica il software di sistema utilizzando una radice di attendibilità hardware. In questo modo è più difficile che gli attacchi di software provochino compromissioni permanenti al sistema operativo e in fase di avvio gli utenti dispongono di una condizione di sicurezza.  Ogni fase di Avvio verificato ha una firma crittografica. Ogni fase del processo di avvio verifica l'integrità della fase successiva, prima di eseguire il codice. A partire da Android 7.0, l’avvio completo di un dispositivo compatibile con un bootloader bloccato procede solo se il sistema operativo soddisfa i controlli di integrità.  A partire da Android 8.1, le implementazioni dei dispositivi con più di 1GB di RAM devono supportare l’Avvio verificato per l'integrità del dispositivo. Gli algoritmi di verifica utilizzati devono essere efficaci come le raccomandazioni correnti del NIST per algoritmi hash (SHA-256) e le dimensioni delle chiavi pubbliche (RSA-2048).  Lo stato di Avvio verificato è utilizzato come input nel processo di derivazione delle chiavi di crittografia del disco. Se lo stato di Avvio verificato cambia (ad esempio, l'utente sblocca il bootloader), l’hardware sicuro impedisce l'accesso ai dati utilizzati per derivare le chiavi di crittografia del disco.  L’Avvio verificato su dispositivi compatibili con sistema operativo Android 8.0 e versioni successive consente la protezione anti-rollback. Ciò significa che una compromissione del kernel (o un attacco fisico) non può inserire una versione del sistema operativo meno recente e più vulnerabile in quello attuale ed eseguire l’avvio. Inoltre, lo stato di protezione anti-rollback è memorizzato anche nella memoria antimanomissione.  Le aziende possono controllare lo stato dell’Avvio verificato utilizzando [l’attestazione chiave KeyStore.](https://developer.android.com/training/articles/security-key-attestation.html) Ciò consente di recuperare una dichiarazione firmata dall’hardware sicuro che attesta molti attributi dell’Avvio verificato insieme ad altre informazioni sullo stato del dispositivo. L’attestazione chiave KeyStore è richiesta per dispositivi forniti dotati di sistema operativo Android 8.0 e versioni successive.  È possibile avere ulteriori informazione sull’Avvio verificato [qui.](https://source.android.com/security/verifiedboot/) |