

# Sicurezza e Sandbox Android

Moisè Lorenzo

Brocanelli

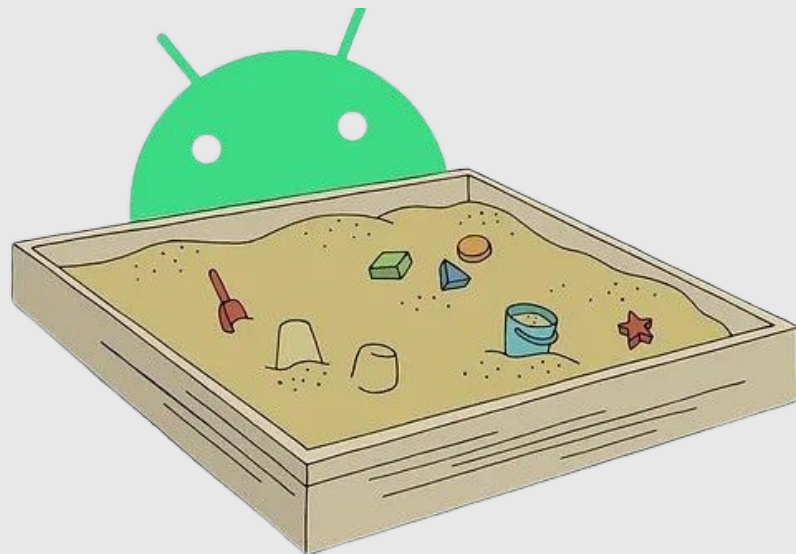
Tommaso

Nicolini Tommaso

# Cos'è la Sandbox su Android?

La **sandbox** è una tecnica di sicurezza implementata in **Android** per isolare ogni applicazione in un ambiente protetto, limitando l'accesso a risorse sensibili e prevenendo danni al sistema operativo principale.

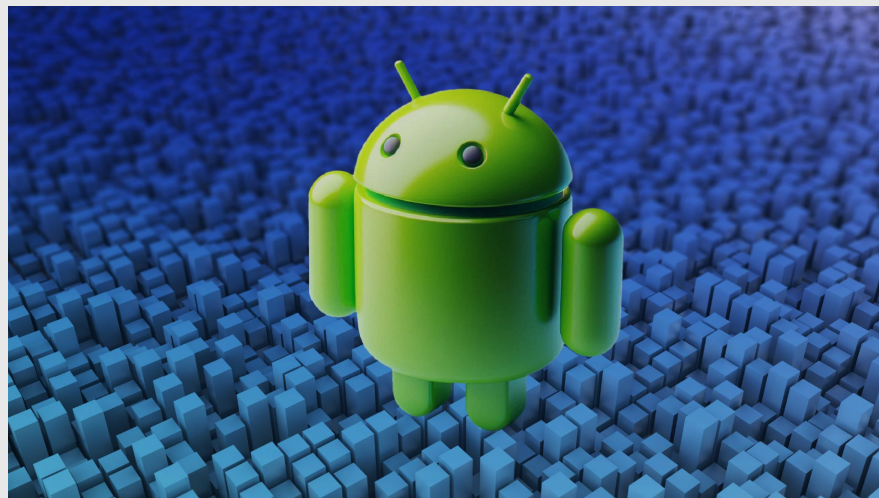
- **Ambiente isolato:** Ogni applicazione Android viene eseguita in un "contenitore" virtuale separato, che non ha accesso diretto ai dati o alle risorse di altre app o del sistema.
- **Protezione avanzata dei dati:** La sandbox impedisce che un'app compromessa possa accedere ai dati di altre app (come contatti, SMS, foto o informazioni bancarie) o modificare file sensibili del sistema operativo.
- **Contenimento dei rischi:** Anche se un'app è infettata da malware, il danno rimane confinato all'interno della sandbox, evitando che si diffonda ad altre app o al sistema operativo.



# Sistema di permessi

Il sistema di permessi di Android permette agli utenti di controllare quali risorse del dispositivo (fotocamera, microfono, posizione, ecc.) possono essere utilizzate da un'applicazione. Alcune evoluzioni significative di questo sistema includono:

- **Permessi runtime (da Android 6.0):** Gli utenti possono approvare o rifiutare i permessi al momento dell'uso, piuttosto che durante l'installazione.
- **Controllo dettagliato:** Gli utenti possono gestire permessi specifici nelle impostazioni, disabilitando quelli non necessari.
- **Permessi una tantum (da Android 11):** Per risorse sensibili come la posizione o la fotocamera, è possibile concedere un permesso valido solo per una singola sessione.



# Google Play Protect

Google Play Protect è il sistema di difesa integrato di Android contro malware e app dannose. Include diverse funzionalità:

- **Scansione delle app installate:** Analizza regolarmente le app sul dispositivo per identificare comportamenti sospetti.
- **Protezione contro app non verificate:** Quando un utente tenta di installare un'app da una fonte esterna, questo sistema avverte se l'app non è stata verificata.
- **Segnalazione in tempo reale:** Se viene rilevato malware, l'app viene bloccata o rimossa automaticamente.
- **Apprendimento automatico:** Google utilizza algoritmi di machine learning per identificare modelli di comportamento associati a malware.



# Aggiornamenti di sicurezza regolari

Google pubblica patch di sicurezza mensili per correggere vulnerabilità critiche. Questi aggiornamenti sono particolarmente importanti per risolvere problemi come:

- **Vulnerabilità zero-day:** Exploit sconosciuti agli sviluppatori fino al momento della scoperta.
- **Bug critici:** Problemi che potrebbero consentire l'accesso non autorizzato al sistema.

Anche se la distribuzione degli aggiornamenti varia:

- **Pixel:** I dispositivi di Google ricevono aggiornamenti immediati.
- **Altri produttori:** Gli aggiornamenti possono essere ritardati o non distribuiti affatto per dispositivi più vecchi.





# Crittografia dei dati

La crittografia è obbligatoria sui dispositivi Android a partire dalla versione 6.0. Include:

- **Crittografia completa del disco:** Tutti i dati sul dispositivo sono crittografati utilizzando AES (Advanced Encryption Standard), rendendoli illeggibili senza una chiave di decrittazione.
- **File-Based Encryption (FBE):** Introdotta con Android 7.0, permette di crittografare singoli file anziché l'intero disco. Ciò migliora le prestazioni e permette al dispositivo di eseguire funzioni di base anche quando è bloccato.



# Secure boot

Secure Boot garantisce che il software caricato durante l'avvio sia firmato e autenticato da un'entità di fiducia (di solito il produttore del dispositivo). In caso di rilevamento di software non autorizzato o manomesso:

- Il sistema può impedire l'avvio del dispositivo.
- Gli utenti vengono avvisati con messaggi di errore o di compromissione.



# Protezione contro exploit

Per prevenire attacchi che sfruttano vulnerabilità di memoria o esecuzione, Android utilizza diverse tecnologie:

- **ASLR (Address Space Layout Randomization):** Sposta casualmente le posizioni di memoria delle librerie, dei processi e delle funzioni, rendendo difficile prevedere dove si trovano i dati critici.
- **DEP (Data Execution Prevention):** Impedisce l'esecuzione di codice non autorizzato da aree di memoria che dovrebbero contenere solo dati.
- **Control Flow Integrity (CFI):** Protegge il flusso di esecuzione del codice, prevenendo attacchi come il "return-oriented programming" (ROP).





# Supporto a TrustZone e hardware sicuro

Android utilizza il **Trusted Execution Environment (TEE)**, una sezione sicura dell'hardware progettata per eseguire operazioni sensibili in un ambiente isolato, al riparo da potenziali minacce come malware o accessi non autorizzati. Questa tecnologia offre una separazione tra il sistema operativo principale e i processi critici, aumentando significativamente la sicurezza dei dati e delle operazioni più delicate. Le sue principali funzioni includono:

- **Gestione sicura delle chiavi crittografiche**, impedendo che siano esposte al sistema operativo principale.
- **Esecuzione protetta di transazioni crittografate**, come pagamenti digitali, riducendo i rischi di compromissione.
- **Verifica dell'integrità del sistema**, assicurando che software e firmware non siano stati alterati.



# Funzioni per la privacy dell'utente

Le versioni più recenti di Android hanno introdotto miglioramenti significativi per proteggere la privacy:

- **Scoped Storage (da Android 10):** Le app possono accedere solo ai file che creano o che sono strettamente necessari per il loro funzionamento.
- **Blocco delle app inattive (da Android 11):** I permessi di app inutilizzate vengono automaticamente revocati. Questo meccanismo impedisce a vecchie app dimenticate di accedere ai dati personali, garantendo un controllo costante sui permessi e riducendo i rischi legati a potenziali vulnerabilità o abusi.



# Conclusione

In conclusione, Android offre un'ampia gamma di caratteristiche di sicurezza progettate per proteggere gli utenti e i loro dati, come l'architettura sandbox, il sistema di permessi, la crittografia avanzata e strumenti come Google Play Protect. Tuttavia, la natura aperta del sistema operativo e la frammentazione dell'ecosistema rappresentano sfide importanti, che richiedono un impegno costante da parte di Google, dei produttori di dispositivi e degli utenti stessi. Adottare buone pratiche, come mantenere il software aggiornato e installare solo app da fonti affidabili, è essenziale per sfruttare al meglio le difese integrate di Android e garantire un'esperienza sicura.