mobisec

MOBISEC

RISULTATI TEST MOBILE APP

SETTORE FINANCE

mobisec.com

mobisec

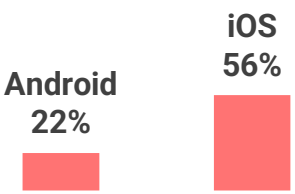
SINTESI DEI RISULTATI

EXECUTIVE SUMMARY

67%

È la percentuale di test falliti dalle applicazioni Android e iOS per comunicazioni non sicure sulla rete.

Circa 7 app su 10 (sia iOS che Android) concedono permessi superiori a quanto necessario.



Test falliti per debolezze nelle librerie di terze parti impiegate.

VOTATI ALLA SECURITY

SU DI NOI

Fondata nel 2015, Mobisec si è occupata fin dal principio di **cybersecurity applicativa,** quando tutti erano concentrati sulla sicurezza infrastrutturale, sulla digitalizzazione dell'azienda e sullo spostamento della gestione aziendale sul cloud.

Proprio quest'ultimo trend porta con sé un aspetto fondamentale: la liability relativa alla sicurezza infrastrutturale passa sempre di più nelle mani di hyperscaler e cloud service provider; ciò rende i datacenter e il network particolarmente resilienti, mentre lascia fortemente esposto il mondo logico-applicativo.

Siamo nati proprio per rispondere alle esigenze di sicurezza di un mondo sempre più connesso, sviluppando competenze e conoscenze uniche in ethical hacking e innovazione. Offriamo soluzioni su misura per fornire sicurezza e serenità a chi gestisce in azienda la cybersecurity degli applicativi, dei dispositivi mobili e dell'IoT.

La nostra missione è ridurre i rischi e le preoccupazioni dei clienti con un approccio innovativo alla sicurezza mobile.

mobisec

L'INDUSTRY DELL'ANALISI

FINANCE

Il settore Finance è da sempre molto attenzionato dal legislatore che impone la compliance a una serie di regolamenti per tutelare gli interessi di correntisti e investitori, come la normativa DORA (Digital Operations Resilience Act) che entrerà in vigore a gennaio 2025.
Spesso, tra tutti gli asset digitali che banche e altri istituti di credito devono gestire, le app mobile vengono trascurate, ma ci si dimentica che **oggi lo smartphone è la porta di ingresso del cliente alla propria banca e, quindi, ai propri risparmi**.

Da qui la volontà di approfondire e verificare lo stato dell'arte di questo settore, che coinvolge milioni di italiani in azioni quotidiane.

E se è vero che la sicurezza digitale di ogni singolo utente finale è data (anche) dalla somma di tutte le singole applicazioni che troviamo all'interno degli smartphone, i player del settore finance hanno la loro quota di responsabilità in questo senso.

LA NOSTRA ANALISI

OBIETTIVI

L’obiettivo di questa indagine, che prende in considerazione diverse industry, è quello di stimare il livello base di sicurezza che esprime un campione selezionato di applicazioni mobile scaricate e installate su milioni di device nel nostro Paese, attraverso un set di test di sicurezza previsti dall’OWASP MASTG, l’organismo di riferimento quando si parla di sicurezza delle applicazioni.

In questo documento ci concentriamo sulle **app mobile** delle principali aziende italiane del settore **Finance**.

NOTA: Per ragioni deontologiche, di riservatezza e di approccio ai test, sono state escluse dai risultati della presente analisi tutte le applicazioni delle aziende già nostre clienti.

OWASP

MASVS E MASTG

Nell’affrontare questa serie di test abbiamo fatto riferimento ai massimi organismi e alle più aggiornate metodologie internazionali.

OWASP

Open Worldwide Applications Security Project è un progetto open source che ha lo scopo di formulare linee guida, strumenti e metodologie per migliorare la sicurezza delle applicazioni informatiche. È considerato l’organismo di riferimento per ciò che concerne gli approcci da tenere quando si tratta di testare la sicurezza delle applicazioni.

Nello specifico, nelle analisi che seguono abbiamo fatto riferimento al progetto MAS (Mobile Application Security) che si compone di diversi elementi tra cui:

MASVS

Mobile Application Security Verification Standard è lo standard di riferimento per la sicurezza delle applicazioni mobile; i gruppi di valutazione sono STORAGE, CRIPTOGRAPHY, AUTHORIZATION and AUTHENTICATION, NETWORK, PLATFORM, CODE, RESILIENCE e PRIVACY.

MASTG

È l’acronimo che identifica la Mobile Application Security Testing Guide, cioè il manuale che raccoglie tutti i test per valutare se un app mobile aderisce alle linee guida stabilite dal MASVS.

OWASP

I TEST MASTG

I test previsti dal protocollo MASTG sono numerosi e puntano ad un altissimo livello di profondità e precisione; il nostro obiettivo in questa fase è stato selezionare quelli che ci consentissero una valutazione a tutto tondo del livello di sicurezza dell'applicazione mantenendo allo stesso tempo una relativa velocità di esecuzione. In altre parole, ci siamo calati nei panni di un hacker che, nella fase preliminare all'attacco, mira a una visione rapida e generale dei possibili punti di accesso a una struttura, in questo caso un'applicazione mobile, per identificare la preda perfetta.

Abbiamo deciso di approfondire i nostri test su due ambiti particolarmente sensibili: Network e Code, dei quali abbiamo svolto rispettivamente 3 e 2 test, a differenza degli altri che ne prevedono 1. La nostra scelta deriva dal fatto che la sezione Network si concentra su come devono essere trasmessi i dati sensibili cioè quei dati che se intercettati potrebbero creare enormi danni all'utente finale e, conseguentemente, al proprietario dell'applicazione; la sezione Code, d'altro canto, analizza gli ambiti dove, statisticamente, si nasconde la maggior parte delle vulnerabilità e dei punti di accesso sfruttati dagli attaccanti.

Ogni sezione del MASTG che abbiamo incluso nella nostra analisi comprende lo stesso test identificato da due codici numerici diversi, questo perché i test vengono sempre svolti sia per iOS che per Android e, sebbene puntino allo stesso obiettivo richiedono procedure diverse.

OWASP

IL SET DI TEST SELEZIONATI

TESTING CUSTOM CERTIFICATE STORES AND CERTIFICATE PINNING

Abbiamo la garanzia che l'nterlocutore col quale scambiamo i nostri dati sensibili sia sempre lo stesso? Con questo test verifichiamo che nessun malintenzionato si possa sostituire al nostro interlocutore reale.

TESTING DATA ENCRYPTION ON THE NETWORK

I nostri dati sensibili, quando viaggiano in rete, sono crittografati? Con questo test verifichiamo che le informazioni scambiate in rete, soprattutto se confidenziali, non siano trasmesse in chiaro.

KEYBOARD CACHE IS DISABLED FOR TEXT INPUT FIELDS

Abbiamo la garanzia che i dati che inseriamo nei campi di testo delle applicazioni vengano cancellati dalla memoria del dispositivo? Con questo test verifichiamo che vengano memorizzati solo quando e dove necessario.

TESTING FOR APP PERMISSIONS

I permessi che diamo alle applicazioni sono sempre sicuri e coerenti con i servizi forniti? Con questo test verifichiamo l'effettiva coerenza tra il servizio offerto e i permessi richiesti.

OWASP

IL SET DI TEST SELEZIONATI

TESTING ENFORCED UPDATING

Siamo certi che l'applicazione sia sempre aggiornata garantendo la massima protezione? Con questo test verifichiamo che l'applicazione forzi l'aggiornamento all'ultima versione per poter funzionare.

CHECKING FOR WEAKNESSES IN THIRD PARTY LIBRARIES

Possiamo fidarci del livello di sicurezza delle librerie utilizzate per lo sviluppo dell'applicazione? Con questo test verifichiamo che le librerie di terze parti che vengono richiamate dall’app siano sufficientemente sicure.

TESTING THE CONFIGURATION OF CRYPTOGRAPHIC STANDARD ALGORITHMS

Qual è il grado di complessità degli algoritmi crittografici e della mia applicazione? Con questo test verifichiamo che gli algoritmi usati siano adeguatamente complessi e rispettino gli standard di mercato.

MAKING SURE THAT THE APP IS PROPERLY SIGNED

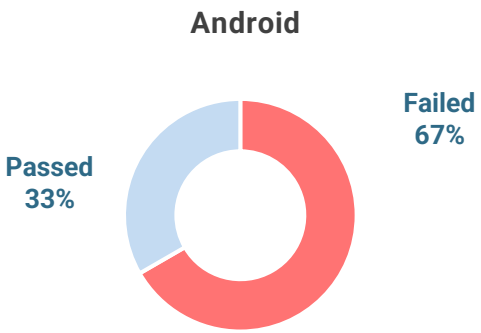
Le firme digitali nei certificati sono attendibili? Con questo test verifichiamo che siano presenti, crittografate e non falsificabili.

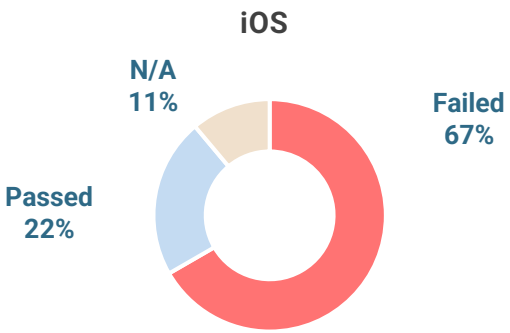
CUSTOM CERTIFICATE STORES AND CERTIFICATE PINNING

MASVS-NETWORK-1
(MASTG-TEST-0022 / 0068)

Controlliamo che il dispositivo si autentichi correttamente agli endpoint di rete verificando che nell'applicazione sia incorporato lo stesso certificato presente nel server così che, al momento del collegamento, la connessione viene accettata solo se i due certificati corrispondono.

I rischi, fallendo questi test, sono di esporsi ad attacchi di ***Sniffing*** o di tipologia ***Man in the Middle (MITM)***, dove un malintenzionato può frapporsi tra client e server modificando il flusso, o di ***Server Spoofing***, dove l'attaccante finge di essere un server trafugando quindi i dati inviati dal client.





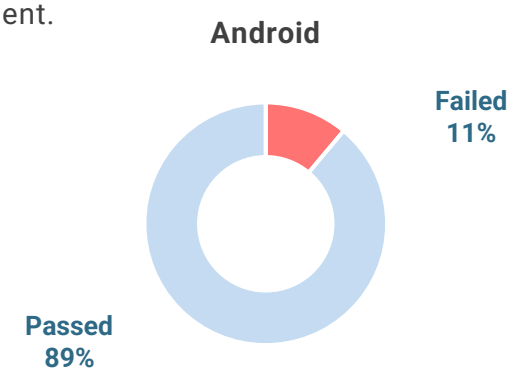
Esiste un elemento interessante legato al *pinning*: OWASP non obbliga ad usare sempre questa tecnica, ma il MASTG include dei controlli specifici. Nella pratica l'utilizzo è consigliato, ma senza abusarne poiché i rischi di compromissione sono alti. Google e Apple ne hanno semplificato le procedure al punto da renderla una best practice comune. **Pur essendo una valida scelta, oggi si opta per tecniche più moderne come la certificate transparency**.

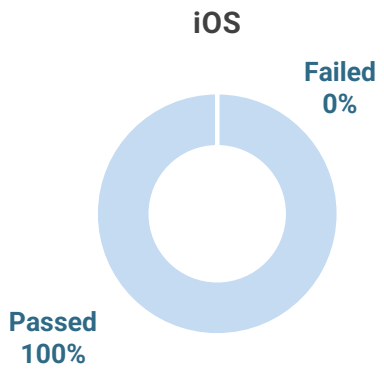
DATA ENCRYPTION ON THE NETWORK

MASVS-NETWORK-2 (MASTG-TEST-0019 / 0065)

Il terzo test della famiglia Network controlla che il traffico dati tra l'applicazione e l'endpoint, già verificato con i test precedenti, avvenga utilizzando i protocolli HTTPS (Hyper Text Transport Protocol Secure) e TLS (Transport Layer Security); inoltre verifica l'aggiornamento di questi protocolli all'ultima versione garantendo un adeguato sistema di crittografia.

I rischi, fallendo questi test, sono di esporsi ad attacchi di ***Sniffing*** o di tipologia ***Man in the Middle (MITM)***, ad esempio sfruttando tecniche di ***downgrade*** delle comunicazioni, dove un malintenzionato può frapporsi tra client e server modificando il flusso, o di ***Server Spoofing***, dove l'attaccante finge di essere un server trafugando quindi i dati inviati dal client.





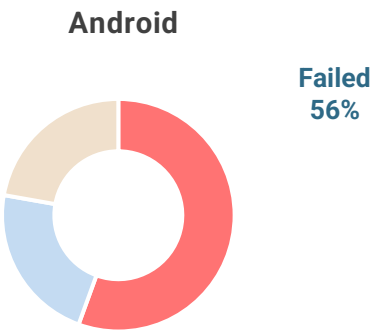
Ad oggi bisognerebbe sempre utilizzare il protocollo https, ma in alcuni casi rimangono aperte porte all'http. Di per sé potrebbe non essere un rischio, a patto di configurare correttamente tutte le comunicazioni e i server, altrimenti si esporrebbe l'app ad attacchi. Nei casi in cui il test fallisce, non si sta utilizzando il **migliore approccio di *fallback***: se un server cambiasse configurazione implementando opzioni non sicure, l'app accetterebbe di continuare a comunicarci.

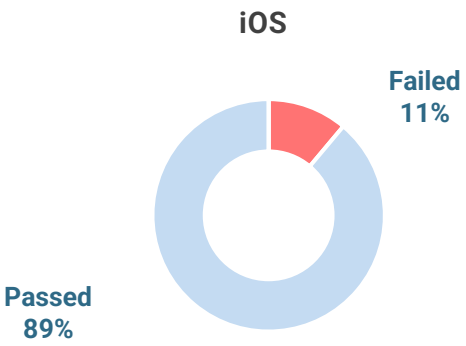
KEYBOARD CACHE IS DISABLED FOR TEXT INPUT FIELDS

MASVS-STORAGE-2
(MASTG-TEST-0006 / 0055)

In questa selezione di test del gruppo «*Storage*» abbiamo verificato se la Keyboard Cache è abilitata per l'input nei campi di testo, cioè se l'app completa in automatico determinate informazioni (potenzialmente sensibili, come utente e password) nei campi di login.

Il rischio è di **esporre dati sensibili** in posizioni accessibili e, quindi, potenzialmente passibili di **esfiltrazione** da parte di malintenzionati.





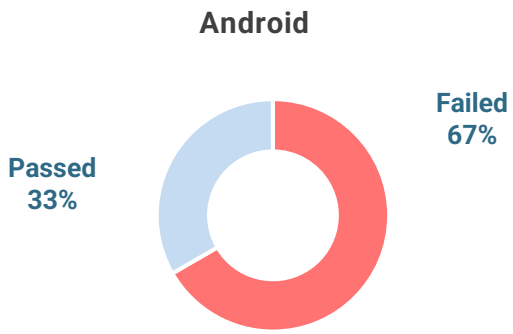
Sebbene il problema della gestione dei dati immessi dagli utenti sia comune tra Android e iOS, i risultati dei test hanno denotato come il sistema operativo più aperto tra i due, **Android, risulti di fatto anche quello in cui c'è meno attenzione e controllo sulla gestione della privacy** dei dati degli utenti.

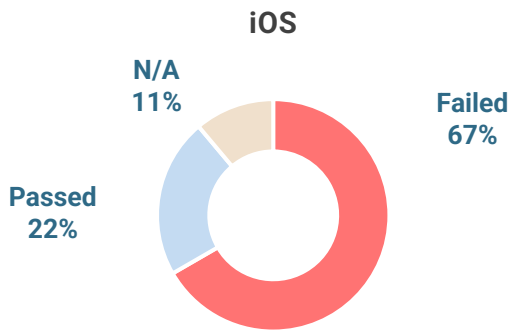
APP PERMISSIONS

MASVS-PLATFORM-1 (MASTG-TEST-0024 / 0069)

In questo set di test del gruppo «Piattaforma» abbiamo verificato se i permessi richiesti dalle applicazioni sono coerenti con l'utilizzo dell'app stessa. Ad esempio, se viene richiesto l'accesso alla fotocamera, alla libreria foto, ai contatti, alla posizione, etc.

Il rischio è di una potenziale **violazione della privacy**, concedendo l'autorizzazione ad informazioni sensibili all'insaputa dell'utente, sfociando in alcuni casi in una non conformità alle politiche degli store con conseguente rimozione dell'applicazione dagli Store ufficiali.





La maggior parte dei permessi rilevati come «non necessari» all'interno delle applicazioni in scope, erano permessi deprecati o inutilizzati. Sia Google che Apple negli ultimi anni stanno apportando importanti modifiche alla gestione dei permessi per tutelare la privacy degli utenti, andando a gestire in maniera più granulare ciò che le app possono fare. **Nonostante ciò, uno sviluppo non corretto dell'applicativo porta a significativi rischi per la tutela della privacy e dei dati degli utenti.**

ENFORCED UPDATING

MASVS-CODE-2
(MASTG-TEST-0036 / 0080)

Con i test «Codice» ci assicuriamo che l'applicazione forzi l'utente a scaricare sempre e solo l'ultima versione disponibile, questo perché un'applicazione regolarmente aggiornata garantisce una user-experience ai massimi livelli
soprattutto sotto l'aspetto della sicurezza informatica.

Un'applicazione non aggiornata è maggiormente esposta ad attacchi che sfruttano **vulnerabilità note** per eseguire malware o prendere il controllo del dispositivo senza considerare i problemi di compatibilità e una user-experience non adeguata.

Android **iOS**

Le applicazioni sia Android che iOS che hanno visto aggiornamenti sostanziali durante il periodo della nostra analisi non è significativo per presentare dei risultati attendibili, pertanto questo test verrà utilizzato come riferimento per le versioni successive del presente documento

Allertare l'utente circa un importante aggiornamento è più di una best practice, essendo uno **strumento fondamentale per mantenere il proprio bacino di utenti sempre allineato alle policy di sicurezza più aggiornate**.

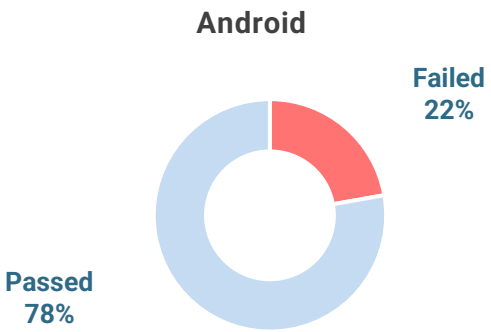
Gli scenari Android e iOS saranno presentati con l'aggiornamento del presente documento, nei prossimi mesi.

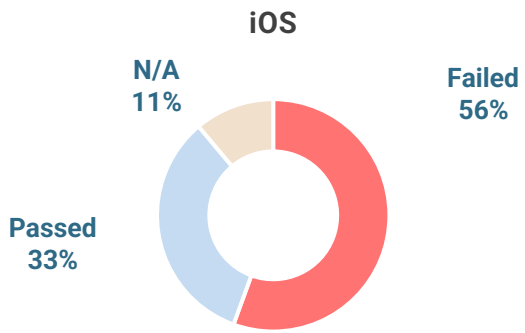
WEAKNESSES IN THIRD PARTY LIBRARIES

MASVS-CODE-3 (MASTG-TEST-0042 / 0085)

Al fine di ottimizzare i tempi di produzione, è pratica comune per gli sviluppatori, ricorrere all'uso di porzioni di codice (librerie) create da terzi e disponibili online: i test del gruppo «Codice» verificano che la sicurezza di tali librerie sia rispettata.

I rischi possono essere legati all'esecuzione di **codice malevolo** nascosto, non rilevato, o all'intrusione di malintenzionati che, **elevando i privilegi**, possono prendere pieno controllo del dispositivo accedendo a tutte le informazioni in esso contenute.





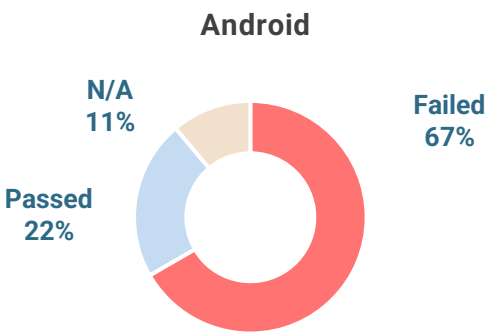
Nonostante il continuo *shift-left* della sicurezza, manca una vera applicazione delle best practice da parte degli sviluppatori **che non mantengono aggiornate librerie di terze parti e framework, causando una continua presenza di vulnerabilità note all'interno delle app**.
Bisogna però riconoscere che è un valore meno preoccupante (almeno per Android) rispetto a quanto riscontrato in altre industry, probabilmente per il modello di business che impone controlli più severi in questo senso.

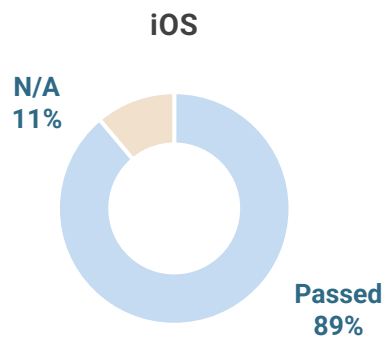
CONFIGURATION OF CRYPTO STANDARD ALGORITHMS

MASVS-CRYPTO-1
(MASTG-TEST-0014 / 0061)

Nel gruppo «Crypto» sono presenti i test per la verifica degli algoritmi crittografici utilizzati dall'applicazione per lo scambio dei dati. In particolare ci si assicura che non siano obsoleti e che la complessità della cifratura sia elevata.

Più la cifratura è debole più aumentano l'esposizione a ***exploit*** con conseguente decrittazione dei dati e violazione della privacy.





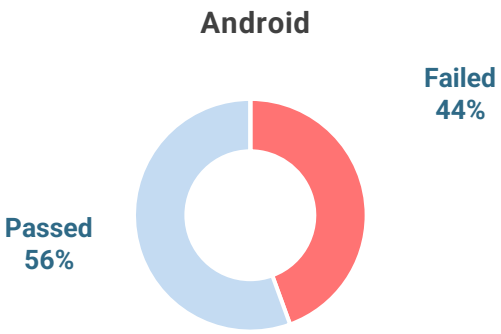
Molte librerie, soprattutto open source e legate al mondo Android, ancora fanno affidamento a metodi di cifratura deboli e deprecati per la messa in sicurezza di file e contenuti a causa di un mancato aggiornamento corretto dell'app in fase di sviluppo. Apple ha il vantaggio di poter controllare a monte il codice eseguito nei suoi dispositivi, portando un **maggior controllo e standardizzazione con l'utilizzo di tecnologie moderne che si propagano all'interno del loro intero ecosistema.**

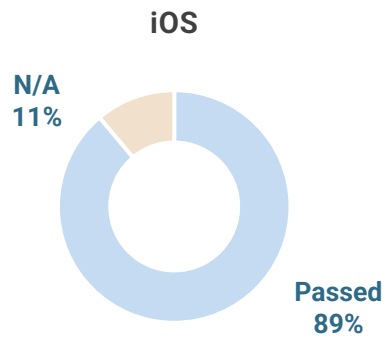
APP IS PROPERLY SIGNED

MASVS-RESILIENCE-2 (MASTG-TEST-0038 / 0081)

Il gruppo «Resilienza» contiene i test che verificano i certificati delle firme digitali, la lora attendibilità e il loro livello di sicurezza nella cifratura. Un certificato di firma adeguato garantisce l'autenticità, l'integrità e la riservatezza delle informazioni scambiate.

I problemi derivanti da una firma non corretta possono portare all'inserimento di **software malevoli** o alla modifica non autorizzata dell'applicazione.





iOS usa sempre automaticamente le ultime impostazione disponibili e gli sviluppatori sono portati a supportare solo le ultime versioni dell'OS. Android spesso supporta versioni dell'OS molto datate a causa di una maggior eterogeneità dei suoi dispositivi, sia in termini hardware che software, **richiedendo agli sviluppatori di usare metodi di firma non aggiornati – e quindi non sicuri – per permettere alle vecchie versioni degli OS di controllare l'app prima di installarla**.

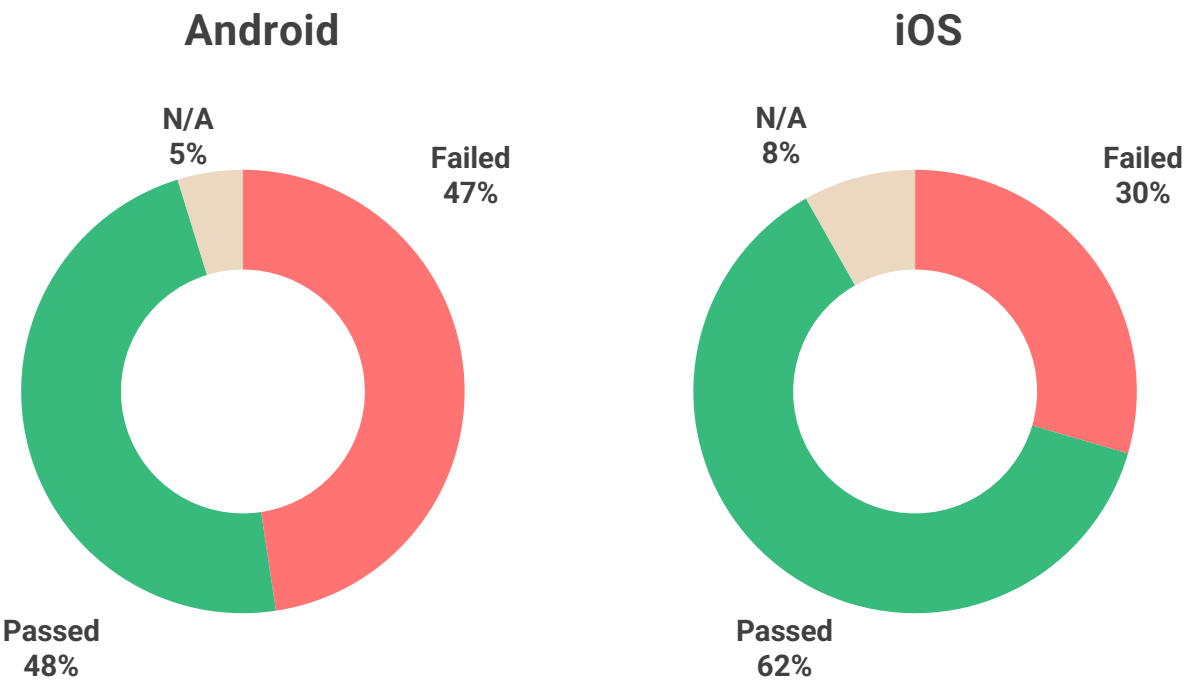
RECAP

I SISTEMI OPERATIVI A CONFRONTO

Da questa nostra analisi, seppur rapida e senza la presunzione di esplorare le dinamiche più profonde delle app, emergono indicazioni importanti: esistono alcune best practice che vediamo condivise tra Android e iOS, dove appunto gli esiti dei test sono positivi per entrambi gli OS e tra le diverse App testate, denotando quindi approcci simili sulle specifiche tematiche.

In generale, Android richiede maggiore controllo da parte dei developer, non perché non sia sicuro di per sé, anzi per certi aspetti potremmo definirlo più sicuro rispetto ad iOS, ma l'ecosistema ha una eterogeneità di device tale da prestare il fianco a meccanismi poco virtuosi dal punto di vista della security.

Alcuni approcci, prerogativa di iOS (ad esempio la gestione della cache o delle firme), portano a risultati più performanti in termini di sicurezza.



I dati relativi ad iOS non comprendono i risultati del test «Enforcement Updating» (MASTG-TEST-0080)

mobisec

staysafe@mobisec.com

Mobisec

Viale della Repubblica 22/III
Villorba (TV)

4010 Moorpark Ave
San Jose, CA 95117

mobisec.com

RESTIAMO IN CONTATTO.