ZEBRA

Consumer o enterprise?

Panoramica

Questo libro bianco presenta un breve documento di sintesi (i dati a supporto sono disponibili su richiesta) delle problematiche che i clienti si trovano a dover affrontare quando cercano di utilizzare dispositivi consumer in applicazioni enterprise. Anche se non riguardano prodotti consumer o di vendor specifici, molte delle affermazioni riguardano Apple in quanto presenta una piattaforma/un modello operativo decisamente particolare. Il presente documento non deve in alcun modo essere considerato una condanna dei dispositivi consumer. Il documento si prefigge di promuovere la "consapevolezza" dei compromessi fatti sia dai produttori enterprise che da quelli consumer.

Coloro che prendono in considerazione dispositivi consumer in applicazioni enterprise dovono considerare quanto segue:

- La mia soluzione sarà sicura e in grado di tutelare la privacy dei dati?
- Supererà realisticamente l'usura di un caso d'uso aziendale?
- La soluzione (vendor, dispositivo, accessori) è in grado di soddisfare i requisiti del mio ciclo di vita?
- Sto dando al reparto IT la possibilità di gestire/amministrare adeguatamente il portafoglio di dispositivi?
- Conosco a fondo il fornitore e so che mi supporterà adeguatamente quando le cose vanno in modo diverso dal previsto?
- Ho la certezza che la soluzione sarà sufficientemente affidabile da non intaccare la produttività dei dipendenti o l'esperienza del cliente?
- Ho davvero passato al setaccio le problematiche che accompagnano una soluzione in più pezzi?
- La soluzione soddisfa davvero le esigenze funzionali presenti e future (prestazioni wireless, scansione di codici a barre, audio, temperatura ecc.)?
- Ho preso in considerazione questioni secondarie come il furto di dispositivi?
- Il mio fornitore mi consentirà di pianificare adeguatamente in anticipo? (per es. visibilità della tabella di marcia)
- I miei sviluppatori e gli ISV di terze parti avranno un adeguato accesso alla programmazione (API)?
- Il mio piano mi consente di consolidare o unificare l'ambiente del sistema operativo?

Consumer o enterprise?

AGGIORNAMENTI DEL SISTEMA OPERATIVO CONTROLLATI DAGLI UTENTI O DAL REPARTO IT

L'esperienza dei consumatori ha a che fare con la praticità e il controllo da parte degli utenti finali. L'esperienza enterprise, invece, ha a che fare con la massimizzazione della produttività e il controllo da parte del reparto IT. Nel modello consumer, gli aggiornamenti del sistema operativo vengono inoltrati agli utenti finali, saltando il reparto IT. Quando vengono inoltrati gli aggiornamenti, gli utenti finali hanno la facoltà/possibilità di aggiornare o di ignorare.

In diversi casi i clienti hanno cercato di bloccare gli aggiornamenti dei dispositivi dei dipendenti tramite filtri di URL proxy. Sfortunatamente, sono stati aggiunti URL di download e i dipendenti sono riusciti comunque ad aggiornare i propri dispositivi. Gli aggiornamenti hanno provocato incompatibilità fra le applicazioni e/o un ambiente OS frammentato. Sfortunatamente, una volta caricati gli aggiornamenti non c'è stato modo di ripristinare la versione precedente del sistema operativo.

Il paradigma enterprise è decisamente diverso. I clienti ottengono gli aggiornamenti da Zebra. Gli aggiornamenti vengono caricati in un MDM su cui il reparto IT ha il controllo completo. Il reparto IT stabilisce quando (spesso durante le ore di inattività per ridurre il carico della rete negli orari di punta) e quali dispositivi ricevono gli aggiornamenti (per es. attraverso una distribuzione progressiva per selezionare le strutture al fine di ridurre i guasti catastrofici). Poiché il reparto IT ha la capacità di eseguire "aggiornamenti incustoditi", la transazione è indipendente e trasparente per l'utente finale. Il reparto IT ha ovviamente la possibilità di introdurre una nuova versione o di ripristinarne una precedente in caso di problemi.

PRESTAZIONI WI-FI

Connettività di base oppure mission-critical

Per le prestazioni Wi-Fi esiste una netta distinzione fra proposte consumer ed enterprise. I dispositivi consumer operano in genere in ambienti AP scarsamente popolati, il che significa che l'efficienza del roaming AP di solito non rappresenta un aspetto significativo. Un roaming scadente può portare a una variazione significativa della latenza, il che può incidere notevolmente sui tempi di risposta della voce e delle applicazioni, con conseguente riduzione della produttività dei dipendenti.

I vendor di soluzioni consumer spesso scendono a compromessi sulla qualità del Wi-Fi in cambio di una riduzione del costo e delle dimensioni. Per esempio, i dispositivi Zebra in genere forniscono antenne a diversità commutata. L'utilizzo di due antenne anziché una incide sulle dimensioni e sul costo ma fornisce una robusta connettività Wi-Fi grazie a una commutazione trasparente sull'antenna ottimale. In questo modo si eliminano i cosiddetti effetti "fantasma" che riducono la connettività in base alla posizione della mano o della testa rispetto al dispositivo (cosa che in passato ha rappresentato un problema con i dispositivi Apple sulla rete cellulare). Inoltre, le antenne di diversità mitigano l'impatto dei riflessi RF (per es. il multipercorso) che creano ampie fluttuazioni della connettività e risultano pervasivi in ambienti aziendali interni.

Inoltre, via via che le reti Wi-Fi diventano sempre più congestionate e le interferenze sempre più prevalenti nella banda da 2,4 GHz, la necessità di una robusta banda da 5 GHz diventa sempre più impellente. Apple non ha introdotto il supporto dei 5 GHz per i propri dispositivi palmari fino alla quinta generazione. A differenza dei dispositivi consumer, molte imprese utilizzavano già i 5 GHz per una maggiore capacità e per evitare interferenze sulla banda da 2,4 GHz. Le prestazioni dei 5 GHz, tuttavia, possono variare. Come riportato in uno studio Gartner sulla valutazione degli iPad Apple, "a 5 Ghz, l'organizzazione IT avrà bisogno del 300% in più di punti di accesso" (a causa delle prestazioni scadenti). Il rapporto è acquistabile da Gartner.

DIMENSIONI DELLO SCHERMO

Per una maggiore produttività

I clienti aziendali chiedono dimensioni dello schermo sempre più grandi (pur mantenendo sempre un equilibrio con la portabilità). Un cliente ha riferito di essere riuscito ad appiattire l'interfaccia utente da 6 livelli a 2 grazie al touchscreen più grande. Questo ha portato a un aumento della produttività dei dipendenti. Gli schermi più grandi hanno inoltre reso possibile l'utilizzo del funzionamento verticale e orizzontale.

Quando Apple ha effettuato la migrazione dei propri prodotti dalla quarta alla quinta generazione, ha modificato dimensioni dello schermo e rapporto di aspetto. Gli schermi più recenti sono da 4,0" con un rapporto di aspetto pari a 16:9. L'MC40, invece, ha uno schermo da 4,3". A prima vista la differenza (da 4,0" a 4,3") sembra trascurabile; occorre tuttavia tenere presente che l'area dello schermo è una funzione esponenziale della diagonale. Pertanto, l'MC40 ha un'area dello schermo superiore del 19,3% rispetto ai dispositivi Apple di quinta generazione. Inoltre, sulla base del feedback ricevuto dai clienti aziendali, nel 2014 Zebra ha lanciato un prodotto con uno schermo da 4,7", il che significa un'area superiore del 38,1% rispetto ai prodotti Apple di quinta generazione.

VOLUME DEI DISPOSITIVI
Sled in 2 pezzi oppure integrati

I dispositivi consumer senza componenti aggiuntivi periferici sono in genere più piccoli e leggeri delle soluzioni enterprise completamente integrate. Tuttavia, quando provvista di uno sled per aggiungere la funzionalità di pagamento, ulteriore capacità della batteria e/o imaging per la lettura di codici a barre, la soluzione in 2 pezzi di classe consumer spesso diventa più grande della configurazione integrata di classe enterprise.

Per esempio, un iPod Touch di quarta generazione ha un volume molto compatto (circa 47 mm^3). Quando dotato di uno sled Infinite Peripherals per aggiungere la scansione di codici a barre e una capacità della batteria paragonabile a quella dell'MC40, il volume di questa soluzione in 2 pezzi sale a 199 mm^3. Si tratta di un volume superiore a quello dell'MC40 (173 mm^3). Inoltre, la dimensione dello schermo della soluzione basata su iPod (quarta generazione) è di 3661 mm^2, mentre lo schermo dell'MC40 è di 5264 mm^2 (con un'area dello schermo superiore del 43%).

In sintesi, pur avendo una funzionalità equivalente, l'MC40 ha un volume più piccolo del 13,1% e fornisce un'area dello schermo superiore del 43%.

SOLUZIONE CON SLED
Resistenza alle cadute

I dispositivi di classe enterprise sono spesso classificati come “durevoli” o “robusti”. Ci si aspetta che i dispositivi durevoli di classe enterprise siano perfettamente operativi dopo 26 cadute (6 cadute laterali, 8 cadute angolari, 12 cadute sul bordo) da un'altezza di 1,2 metri sul compensato. Zebra ha testato una nota soluzione con sled (che fornisce la scansione di codici a barre e la batteria aggiuntiva) utilizzando il test da 26 cadute. La soluzione (sled e iPod) ha subito 6 guasti di grave entità, come: 1) un pezzo del fermo sinistro si è rotto; 2) entrambi i pulsanti di innesco del volume (sullo sled) non riuscivano a modificare il volume; 3) gli altoparlanti non riuscivano a produrre alcun suono e gli scanner non funzionavano; 4) l'unità non si ricaricava correttamente; 5) un pezzo della fibra ottica LED, nella parte inferiore del dispositivo, era fuoriuscito; 6) verso la parte superiore del dispositivo si percepiva un rumore metallico. L'unità ha inoltre riportato 6 guasti di lieve entità (mancato funzionamento ma funzionalità ripristinata dopo il riavvio).

SOLUZIONE CON SLED
Amperaggio e contatto nominale

In genere i dispositivi consumer non specificano (e risulta difficile determinare) l'amperaggio e il contatto nominale per le soluzioni con sled in 2 pezzi. Si tratta, tuttavia, di articoli con un elevato tasso di guasti nei casi d'uso aziendali. Il pulsante di accensione dell'MC40, per esempio, è omologato per 500.000 cicli, il pulsante di scansione/fotocamera per 1.000.000 di cicli, e l'inserimento della batteria per 2000 cicli (6000 per il terminale).

SOLUZIONE CON SLED
Architettura della batteria

Secondo il feedback ricevuto da Zebra, in una serie di modelli di sled la batteria principale è isolata dalla batteria dello sled (ossia le due batterie non condividono l'alimentazione). In questo modo, per poter disporre di un'unità funzionale è necessario che siano caricate sia la batteria dell'iPod che quella dello sled. Sul mercato sono disponibili diversi sled, perciò i clienti dovranno verificare il funzionamento della batteria della soluzione in corso di valutazione. Tenete presente che, nell'arco del tempo, il funzionamento indipendente della batteria può creare problemi di durata.

ACUSTICA DELL'AUDIO
Livelli di pressione sonora

I dispositivi consumer cercano di essere estremamente sottili, anche se questo significa scendere a compromessi su caratteristiche chiave per l'uso enterprise. Un numero crescente di clienti enterprise è alla ricerca di un dispositivo su cui convergano voce e dati. Gli utenti che operano in interni cercano la convergenza fra dispositivi push-to-talk di tipo tradizionale con dispositivi di raccolta dati. In tutti i casi, le imprese sono alla ricerca di un dispositivo udibile in maniera affidabile dal dipendente in ambienti con un rumore relativamente elevato.

Per ottenere il fattore di forma desiderato, i dispositivi consumer di solito sacrificano il livello di pressione sonora dell'audio (Sound Pressure Level, SPL) e la risposta in frequenza. Zebra ha rilevato che numerosi dispositivi consumer di grande diffusione presentano un SPL inferiore di 9-20 dB rispetto ai dispositivi enterprise di Zebra. Anche se soggettiva e basata in modo non lineare sull'output assoluto, una differenza di 9 dB nei livelli di SPL corrisponde in genere a una percezione di un volume doppio.

CAPILLARITÀ FUNZIONALE DELLO SLED

Scansione di codici a barre integrata

In molti casi, i clienti enterprise desiderano una scansione aggressiva su tutti i dispositivi, tutto il tempo, e una soluzione mPOS solo su alcuni dispositivi e/o esclusivamente in determinati periodi dell'anno. Quando prendono in considerazione le soluzioni con sled, sono costretti a considerare la possibilità di fornire 2 diverse configurazioni con sled (una per la scansione e una per la scansione e il pagamento) oppure di dotare il 100% dei dispositivi con l'opzione più grande e costosa (scansione e pagamento). La maggior parte preferisce avere la scansione integrata nel dispositivo e il pagamento relegato a uno sled.

SLOT DI ESPANSIONE

I clienti enterprise spesso richiedono uno storage rimovibile per il porting/backup dei dati e/o per le espansioni della memoria. I dispositivi Apple non offrono supporti rimovibili (come schede SD, unità flash ecc.)

SUPPORTO NFC

Si tratta di una problematica che riguarda nello specifico Apple, che ha ripetutamente deciso di non supportare la comunicazione NFC. Molti clienti enterprise sono alla ricerca della NFC per leggere marcatori di posizione, abbinare periferiche, leggere i tag dei beni e controllare gli accessi.

FLESSIBILITÀ DEL LAUNCHER

Nel caso dei dispositivi Apple, gli utenti non hanno la possibilità di sostituire o modificare il launcher.

TASSI DI PERDITA

Contrazione/furto dei dispositivi

La domanda aftermarket di dispositivi consumer è estremamente elevata, il che aumenta la motivazione al furto. Nel caso di dispositivi consumer senza batterie intercambiabili, i clienti spesso forniscono due set di dispositivi; mentre il primo è in uso, il secondo si trova in un alloggiamento per ricarica. Secondo quanto riferito dai clienti, i dispositivi nell'area di ricarica spesso vanno persi.

TEMPERATURA

Operativa e di conservazione

I dispositivi consumer presentano in genere una gamma molto limitata di temperature operative e di conservazione. Nel caso dei dispositivi Apple, ad esempio, la temperatura operativa va da 0 a 35 gradi C. Quando il dispositivo si surriscalda, comincia a funzionare in modo difettoso e riporta un punto esclamativo con un messaggio che invita a lasciar raffreddare l'apparecchio. Una serie di clienti ha segnalato questo problema in ambienti relativamente innocui. Per contro, dispositivi di classe enterprise come l'MC65 di Zebra hanno una temperatura operativa compresa fra -10 e 50 gradi C (vale a dire 25 gradi in più rispetto ad Apple). Un cliente ha riferito di essere stato costretto a collocare i dispositivi in un'unità di raffrescamento in loco per ripristinarne il funzionamento. Un altro cliente ha riferito una condizione di surriscaldamento in Texas in novembre, durante una consegna diretta in negozio sperimentale.

È importante tenere presente che si tratta di una specifica di temperatura ambientale. Pertanto, quando il dispositivo viene collocato in uno sled, il calore proveniente da quest'ultimo e la mancanza di un percorso termico esterno adeguato possono ridurre ulteriormente il range di temperature elevate.

Anche la temperatura di conservazione è stata riportata come un problema per i dispositivi Apple. Secondo un cliente, l'esposizione a una temperatura di conservazione minimamente al di là del valore massimo indicato per il dispositivo ha provocato una riduzione permanente della durata della batteria. I valori relativi alla temperatura di conservazione per un dispositivo Apple vanno da -20 a 45 gradi centigradi, mentre i valori della temperatura di conservazione dell'MC65 di Zebra vanno da -40 a 70 gradi centigradi.

CICLI DI VITA DEI DISPOSITIVI ENTERPRISE

I dispositivi consumer devono stare al passo con le ultime mode e tendenze. La vita utile (il tempo trascorso il quale non è più vendibile) tipica di uno smartphone è di 6-9 mesi. I dispositivi Apple vengono generalmente immessi sul mercato ogni 12 mesi. La misura in cui le aziende consumer rendono disponibili dispositivi legacy dopo il lancio iniziale non è definita. I clienti enterprise sono quindi costretti a scegliere fra una soluzione molto costosa che prevede la sostituzione integrale e una rotazione progressiva che risulta complessa dal punto di vista logistico e crea un'implementazione estremamente frammentata.

Nello spazio consumer, la compatibilità con accessori legacy è presa in considerazione, ma in genere non è un requisito essenziale. All'interno di Apple, l'introduzione del connettore Lightning (che ha sostituito il connettore a 30 pin) e le variazioni del fattore di forma introdotte nell'iPhone 5 hanno costretto i clienti enterprise a sostituire integralmente sled, alloggiamenti di ricarica e altri accessori per poter migrare al nuovo dispositivo.

I dispositivi enterprise come quelli di Zebra hanno in genere un ciclo di vita di 3+3 (6 anni) o di 5+5 (10 anni). Il primo termine corrisponde alla disponibilità del dispositivo e il secondo al supporto. Pertanto, nel caso di una soluzione 3+3 i clienti possono acquistare il dispositivo per 3 anni e ricevere assistenza per altri 3 anni (con un ciclo di vita totale di 6 anni).

MANTENERE LA SICUREZZA E LA PRIVACY AZIENDALI

Apple e Google (tramite GMS, Google Mobile Services) sfruttano i dispositivi per promuovere e vendere servizi. Tali servizi richiedono in genere (per esempio tramite un accordo EULA) l'accesso ai dati del dispositivo, cosa che può comportare la violazione delle policy aziendali in materia di privacy e di sicurezza. Per esempio, IBM ha annunciato pubblicamente di aver bandito Siri[1]. Come riportato nell'accordo EULA per Siri, "l'utente accetta e acconsente che Apple, le sue controllate e i suoi agenti trasmettano, raccolgano, eseguano la manutenzione, elaborino e utilizzino queste informazioni, ivi inclusi l'input vocale e i dati utente." Poiché tali dispositivi richiedono la connettività cloud, i clienti sono stati costretti a creare dei buchi nei firewall aziendali. Alcuni clienti Zebra, fra cui diversi retailer di primo piano, hanno dichiarato che non consentiranno la presenza di dispositivi GMS sulla propria rete aziendale a causa di preoccupazioni di questo tipo riguardanti la privacy.

TABELLE DI MARCIA DEI PRODOTTI CONSUMER

Avvolti nel mistero

La privacy e segretezza delle tabelle di marcia sono di vitale importanza per le proposte consumer, ma in diretto conflitto con la pianificazione aziendale e la continuità del servizio. Apple è fiera della segretezza:

- "La mancanza di informazioni mantiene alto l'interesse del pubblico mentre i consumatori formulano varie ipotesi" – Regis McKenna, uno dei consulenti di marketing originari di Apple
- "Senza una tabella di marcia precisa con cui lavorare, molti acquirenti evitano di acquistare prodotti Apple" – Jeff Gamet, MAC Observer

IL MALWARE DEGLI APP STORE

Blocco dei dispositivi (MAM — Mobile Application Management)

Come riportato dalle linee guida NIST in materia di sicurezza mobile, la best practice per la sicurezza consiste nel negare l'accesso agli app store pubblici. Ovviamente, per dispositivi consumer come quelli Apple, l'app store rappresenta una significativa proposta di valore e non può essere disattivato.

Anche se lo store Google Play di Android ha registrato un alto grado di contenuti dannosi, le applicazioni disponibili nell'app store di Apple possono a loro volta violare i dati aziendali. Attraverso applicazioni delle schermate Apple, questo app store permette alle applicazioni di reperire e caricare dati sensibili nei dispositivi.

Ecco alcuni esempi di risorse chiave facilmente accessibili (e quindi vulnerabili) tramite applicazioni iOS legittime:

- Comunicazioni wireless con altri dispositivi
- Rubrica (indirizzi di posta elettronica, note sui recapiti ecc.)
- Calendario
- Identificativo del dispositivo (un ID proprietario assegnato da Apple a ciascun dispositivo)
- Numero telefonico del dispositivo (disattivabile tramite una modifica della configurazione)
- File musicali/video e galleria fotografica
- Cronologia ricerche su Safari
- Cronologia autocompletamento del dispositivo
- Elementi visualizzati di recente su YouTube
- Registri connessioni Wi-Fi
- Microfono e videocamera

[1] http://www.zdnet.com/blog/btl/ibm-bans-siriprivacy-risk-or-corporateparanoia-at-its-best/77843

RIMOZIONE DI SERVIZI INDESIDERATI

Viste le vulnerabilità introdotte dagli app store pubblici, alcuni clienti hanno cercato di rimuovere l'app store di Apple dai dispositivi iOS e hanno segnalato che "continua a tornare".

GESTIONE DELLE APPLICAZIONI MOBILI (MOBILE APPLICATION MANAGEMENT, MAM) — IMPOSSIBILITÀ DI CREARE WHITE-LIST

I dispositivi CLD (Corporate Liable Devices) di solito sono bloccati per quanto riguarda le applicazioni che possono essere caricate ed eseguite. I clienti hanno espresso frustrazione dovuta all'incapacità di creare "white-list" (vale a dire elenchi di applicazioni autorizzate) su dispositivi consumer come quelli che eseguono Apple/iOS (il white-listing è una funzionalità standard di Android/Mx).

PERCEZIONE DELLA NOTORIETÀ DEL BRAND

Scegliete un partner, non un dispositivo

Nel terzo trimestre del 2013, Apple ha venduto 33,8 milioni di iPhone e Samsung ha venduto 88,4 milioni di smartphone. Questo dato corrisponde, su base annua, rispettivamente a 135,2 milioni e 353,6 milioni di unità. Pertanto, Samsung spedisce quasi un milione di unità ogni giorno dell'anno. La distribuzione enterprise di 10.000 unità rappresenta quindi solo l'1% delle spedizioni effettuate in un singolo giorno. Le aziende enterprise, per contro, spediscono in genere meno di 1,5 milioni di unità all'anno. Pertanto, un'opportunità da 10.000 unità rappresenta una significativa opportunità e offre la possibilità di generare un buon livello di notorietà del brand.

Come ha dichiarato da un cliente Zebra, quando scegliamo una proposta consumer scegliamo un dispositivo, non un partner. Questo rispecchia le percezioni espresse di recente in un articolo del Wall Street Journal[3].

SPESE GENERALI PER LA LOGISTICA

Aggiornamenti dei certificati di distribuzione

Per distribuire le applicazioni Apple, dovete iscrivervi al programma di sviluppatori Apple Enterprise (un certificato enterprise che dura 3 anni) e ottenere un certificato di distribuzione. Le applicazioni vengono quindi implementate; tuttavia, alla scadenza del certificato di distribuzione (che dura 1 anno), dovete ricostruire le applicazioni con un certificato rinnovato e quindi provvedere di nuovo all'implementazione. Come riferito da diversi clienti enterprise, le applicazioni installate semplicemente non funzionano (possono funzionare per alcuni giorni fino a che il certificato viene invalidato dal server OCSP di Apple).

RIAVVIO REMOTO

Indipendentemente dal numero di precauzioni adottate, talvolta i dispositivi devono essere riavviati. Il riavvio programmatico del dispositivo richiede l'accesso alle API, raramente disponibile nei dispositivi consumer (per es. nell'iOS Apple). Android/Mx di Zebra, invece, mette le API a disposizione di applicazioni affidabili e firmate per il riavvio programmatico del dispositivo (in genere eseguito da remoto tramite MDM).

GESTIONE DELLA BATTERIA

Mantenimento del tempo di attività

I casi d'uso aziendali spesso mettono l'accento sulla durata della batteria (sia a breve che a lungo termine). In molti casi, i dispositivi consumer (per es. quelli Apple) non hanno la possibilità di sostituire le batterie. In tali casi, i clienti enterprise sono costretti ad acquistare 2 dispositivi al posto di 1 e una batteria sostitutiva. In alcuni scenari la batteria è sostituibile, ma il meccanismo di aggancio non è progettato per cicli ripetuti e spesso si guasta nell'arco del tempo.

"Il progettista Dustin Curtis riferisce di avere condotto un rapido sondaggio con 15 sviluppatori di applicazioni iOS molto diffuse, e che '13 di essi hanno dichiarato di avere un database di contatti con milioni di record. Il database di un'azienda contiene il numero di cellulare di Mark Zuckerberg, il telefono di casa di Larry Ellison e il numero di cellulare di Bill Gates.'"[2]

[2] http://www.pcworld.com/article/250007/path_isnt_only_app_to_upload_store_address_book_data.html
[3] http://blogs.wsj.com/cio/2013/06/12/apple-stilllags-in-enterprise-support/

ACCESSO AI DISPOSITIVI

Per esempio tramite telecomando

Il design della piattaforma iOS di Apple è relativamente chiuso. È vero che questo limita l'esposizione a contenuti nocivi, però limita anche la capacità degli sviluppatori aziendali di aggiungere funzionalità avanzate. Per esempio, una funzionalità enterprise richiesta di frequente è quella di permettere al reparto IT di assumere il controllo del dispositivo dell'utente da una postazione remota. Questa funzionalità viene normalmente utilizzata per scopi di formazione e per la diagnostica. Per consentire questa funzionalità, è necessario concedere a un'applicazione affidabile l'accesso al buffer del display, cosa non disponibile sulle piattaforme Apple. Soluzioni come Android/Mx di Zebra, per contro, permettono ad applicazioni affidabili (con relativa procedura di accesso) di accedere a risorse come il buffer del frame.

In sintesi, il processo di firma di Android permette ad applicazioni affidabili e firmate/autenticate il necessario livello di accesso per attivare funzionalità enterprise.

RISOLUZIONE ULTRAELEVATA

Bilanciare il valore aziendale

I dispositivi consumer stanno migrando verso schermi a risoluzione ultraelevata. Apple, ad esempio, dall'iPad2 all'iPad New è passata da 1024x768 a 2048x1536. È stato segnalato che questa transizione ha richiesto il doppio dei LED per la retroilluminazione e ha portato a un aumento del 68% nella batteria dell'iPad New. Come emerso da uno studio[4], l'efficienza energetica dello schermo si è sensibilmente ridotta (ora serve un'alimentazione superiore di 2 volte e mezzo per la stessa luminosità). Inoltre, le applicazioni che cercano di trarre vantaggio dalla risoluzione ultraelevata sono aumentate di dimensioni (per es. Bjango è passata da 18,3 a 35 MB). Spingere un carico utile superiore può aumentare il costo quando si utilizza un operatore con un modello di prezzi dati stratificato.

È vero che un'elevata risoluzione è importante per i clienti enterprise, ma gli estremi provocati dai dispositivi consumer, che scendono a compromessi su durata della batteria e/o peso, non sono necessariamente vantaggiosi.

GESTIONE DEI FILE

I responsabili IT aziendali spesso desiderano poter visualizzare e gestire file e cartelle all'interno di un dispositivo. Sfortunatamente, il file system iOS di Apple non è aperto. Anche se esistono applicazioni di terze parti, la loro efficacia è limitata a causa dell'architettura iOS.

CRIPTATURA

Il compromesso è l'ottimizzazione delle dimensioni dei file

L'efficienza dell'implementazione della criptatura varia a seconda dell'obiettivo target. Apple e Samsung adottano una criptatura basata sull'hardware. I test condotti da Zebra hanno dimostrato che, per file di grandi dimensioni (per es. 128 MB, come nel caso dei file multimediali), la criptatura dell'hardware Apple è efficace. Tuttavia, per file di piccole dimensioni (1 KB), i test di Zebra hanno dimostrato che l'implementazione della criptatura Zebra è più veloce del 306%. Il presupposto è che la criptatura attraverso l'hardware richieda un'inizializzazione e impostazione che vengono ammortizzate per file di grandi dimensioni ma che incidono sui piccoli file. Anche se la criptatura tramite hardware può essere molto efficace per file multimediali di grandi dimensioni (per es. DRM o film), potrebbe non essere ottimale per i file più piccoli spesso utilizzati in applicazioni aziendali.

STORAGE CENTRALIZZATO

In iOS, le applicazioni sono universi a sé stanti e mantengono il proprio storage, al quale è possibile accedere solo attraverso quella particolare app. Questo complica la condivisione di strutture dati di grandi dimensioni (le app richiedono in genere che venga effettuata un'altra copia). Quando le applicazioni condividono dati, il profilo (per es. la criptatura) della struttura dati originaria potrebbe non essere mantenuto nella struttura copiata, violando così le policy in materia di sicurezza.

I clienti enterprise spesso richiedono uno storage rimovibile per il porting/backup dei dati e/o per le espansioni della memoria. I dispositivi Apple non supportano/offrono supporti rimovibili (come schede SD, unità flash ecc.)

[4] http://www.slashgear.com/ipad-retina-displaysquashes-rivals-but-its-notperfect-20219167/

LA MEMORIA FLASH MLC POTREBBE DANNEGGIARSI CON L'USO PROLUNGATO

La memoria flash viene in genere configurata come cellula multilivello (Multi-Level-Cell, MLC) o monolivello (Single-Level-Cell, SLC). Le configurazioni MLC forniscono in genere una capacità doppia rispetto alla SLC equivalente, ma possono provocare il danneggiamento dei dati nell'arco del tempo. Dopo un utilizzo prolungato ("usura"), i livelli di tensione dei gate flottanti che rappresentano bit di informazioni contenuti nella MLC variano e i bit vengono letti in modo errato.

A causa dei cicli di vita relativamente brevi e dell'utilizzo relativamente benigno (rispetto a quelli enterprise), i dispositivi consumer e alcuni dispositivi enterprise utilizzano una memoria flash MLC. I clienti dovranno convalidare il modello di caso d'uso/ciclo di vita per stabilire la configurazione ottimale della memoria flash.

IMPOSSIBILITÀ DI BLOCCARE I PROFILI DI CONFIGURAZIONE TRAMITE MDM

I dispositivi Apple possono essere configurati utilizzando dei "profili di configurazione" (CP). I profili di configurazione sono file XML come specificato da Apple. Quando un amministratore IT configura un dispositivo con un CP, quest'ultimo può essere: aperto (prontamente modificato), modificato solo con un passcode o bloccato (qualsiasi modifica provoca la cancellazione totale del dispositivo).

Quando si utilizzano profili generati da una MDM, non esiste un metodo equivalente per bloccare il profilo di configurazione. Pertanto, i dispositivi del profilo provenienti da una MDM possono essere facilmente modificati o eliminati da un utente finale.

"UN UNICO SISTEMA OPERATIVO DAL MAGAZZINO AL NEGOZIO", A DIFFERENZA DI QUANTO AVVIENE CON LE PROPOSTE CONSUMER

Un retailer di fascia alta (fra gli altri) ha dichiarato: "Vogliamo un unico sistema operativo dai magazzini al negozio". I magazzini richiedono in genere dispositivi specifici per determinate applicazioni, ed è improbabile che provengano da Apple. Zebra, per contro (e, a nostro avviso, il settore in senso lato) offrirà soluzioni Android dal magazzino al retronegozio, dal negozio a un addetto sul campo.

SCELTA E SELEZIONE

L'importanza della concorrenza

Per quanto riguarda in particolare Apple, questa società ha un portafoglio con un'unica fonte, costituito da tre dispositivi di base: iPod, iPhone e iPad. Non esistono dispositivi specifici per determinate applicazioni; tutti gli usi specifici sono gestiti tramite sled. Per contro, nel marzo 2013 c'erano oltre 48 produttori di dispositivi Android e più di 550 dispositivi disponibili. Questo dato comprende produttori di dispositivi enterprise (Zebra, Honeywell, Bluebird ecc.) e consumer. Questo diverso scenario fornisce alle imprese prezzi più competitivi e tutti i vantaggi derivanti dalla molteplicità delle fonti (per esempio una riduzione del rischio).

ACCESSO LIMITATO ALLE API

Consentire l'accesso enterprise

Per Apple iOS e WP8, le API sono bloccate in modo da ridurre al minimo la superficie di attacco a disposizione di applicazioni nocive. Anche se potenzialmente benefico per i consumatori che scaricano applicazioni sconosciute da fonti sconosciute, questo approccio basato sul blocco limita sensibilmente le funzionalità all'interno di applicazioni affidabili di classe enterprise (molti clienti enterprise desiderano controlli wireless dettagliati o l'accesso a periferiche hardware).

VULNERABILITÀ DEI PORTACHIAVI

I ricercatori dell'istituto Fraunhofer hanno indicato, in una loro pubblicazione, un significativo punto vulnerabile di iOS. Nel sistema operativo iOS, molte password (accesso alla rete VPN, password per l'accesso a Exchange Active Sync, password per la connessione Wi-Fi, posta vocale) sono archiviate nell'apposito portachiavi. Tale portachiavi di iOS è criptato con "materiale" (dati) archiviato localmente sul dispositivo. Un hacker può pertanto estrarre il materiale dal dispositivo e decriptare il portachiavi, rendendo facilmente accessibili le password archiviate. Nota: un aggiornamento di tale analisi è ancora sospeso per l'ultima release di iOS 7.[5]

VULNERABILITÀ DELLA SICUREZZA DI SIRI

Siri è un'applicazione per il riconoscimento vocale dei linguaggi naturali introdotta nell'iPhone 4S. Gran parte del valore di Siri risiede nella capacità di permettere agli utenti di porre quesiti rapidi in un linguaggio naturale. In una configurazione standard

[5] "Fraunhofer researchers circumvent encryption devices iPhone", Latest IT News, 9 febbraio 2011

Siri viene attivata semplicemente premendo un pulsante al di fuori del blocco del dispositivo. Pertanto, in caso di furto o smarrimento del dispositivo, chi entra in possesso di quest'ultimo può accedere istantaneamente a e-mail, contatti e messaggi di testo. È vero che Siri può essere riposizionata al di là del firewall di blocco, ma questo ne ridurrebbe sensibilmente il valore.

FOTOCAMERE CONSUMER PER L'ACQUISIZIONE DI CODICI A BARRE

Zebra in genere definisce due classi di sottosistemi di imaging: “fotocamere” e “imager”. Come si evince dal nome, per “fotocamera” si intende il sistema multifunzione tipico di una fotocamera digitale di classe consumer. I sistemi della fotocamera di solito sono: cromatico (colore), messa a fuoco automatica, conteggio pixel elevato e ampio angolo di visualizzazione, escludendo qualsiasi forma di meccanismo di puntamento all'infuori del mirino. Inoltre, le fotocamere in genere scattano immagini dal retro del dispositivo. Un “imager”, invece, è in genere monocromatico, con messa a fuoco fissa, un basso conteggio pixel con obiettivi per pixel più grandi, un otturatore globale, un angolo di visualizzazione più stretto e comprende un meccanismo di puntamento. Gli imager sono solitamente situati nella parte anteriore del dispositivo (“shooter anteriore”).

Relativamente importanti per un sistema robusto per l'acquisizione di codici a barre sono gli algoritmi di elaborazione del segnale, che servono ad acquisire e decodificare i codici a barre all'interno dell'immagine. I dispositivi Apple che sfruttano la fotocamera per la decodifica dei codici a barre utilizzano di frequente un software per la decodifica del laser rosso. Test empirici del software per il laser rosso hanno riportato quanto segue: frequenti decodifiche errate, limitato supporto delle simbologie e problemi in caso di decodifica di codici a barre danneggiati o degradati.

Per le applicazioni di lettura di codici a barre, il sottosistema con imager presenta una durata superiore, una maggiore sensibilità, una migliore acquisizione (puntatore) e una maggiore immunità rispetto ai tremolii della mano.

CRIPTATURA AI SENSI DELLA NORMA FIPS PER IL WI-FI

Pubblica amministrazione, settore sanitario e alcuni retailer (quelli con interfaccia per farmaci e/o PCI per mPOS) chiedono che i moduli crittografici del dispositivo (vale a dire quelli utilizzati per la criptatura/decriptatura) siano certificati ai sensi della norma FIPS 140-2 Livello 1. Tale livello di FIPS assicura un design ottimale per la pratica commerciale. I moduli crittografici certificati FIPS sono di solito disponibili sia per i dispositivi enterprise che per quelli consumer. Tali moduli, tuttavia, di solito non si applicano alla criptatura dei collegamenti Wi-Fi (ossia riguardano esclusivamente l'utilizzo di applicazioni). Zebra ha offerto in passato lo standard FIPS su prodotti Wi-Fi basati su Microsoft e nel 2014 ha cominciato a offrire lo standard FIPS per il Wi-Fi per una serie di prodotti Android.

Per maggiori informazioni visitate il sito www.zebra.com/mobilecomputers

Sede centrale e Nord America
+1 800 423 0442
inquiry4@zebra.com

Sede Asia-Pacifico
+65 6858 0722
contact.apac@zebra.com

Sede EMEA
zebra.com/locations
mseurope@zebra.com

Sede America Latina
+1 847 955 2283
la.contactme@zebra.com