ZEBRA

Consumer vs Enterprise

Overview

This paper presents a brief executive summary (backup data available upon request) of issues surfaced by customers attempting to use consumer devices in enterprise applications. Though not targeting any specific vendor of consumer products, many of the statements are directed at Apple since it has a very unique platform / operating model. In no way should this document be viewed as a condemnation of consumer devices. The document is designed to bring about "awareness" of the compromises made by both enterprise and consumer manufacturers.

Those considering consumer devices in enterprise applications should consider the following:

- Will my solution be secure & maintain my data privacy?
- Will it realistically survive the wear and tear of an enterprise use case?
- Can the solution (vendor, device, accessories) meet my lifecycle requirements?
- Am I enabling IT to adequately manage / administer the device portfolio?
- Do I have the mindshare of the supplier so as to adequately support me when things don't go as planned?
- Am I confident that the solution will be reliable enough so as not impact employee productivity or customer experience?
- Have I truly vetted out the issues accompanying a multi-piece solution?
- Does the solution truly meet current and future functional requirements (wireless performance, barcode scanning, audio, temperature…)?
- Have I considered secondary issues like device theft?
- Will my supplier enable me to adequately plan ahead? (e.g. roadmap visibility)
- Will my developers and third party ISV's have adequate programming (API) access?
- Does my plan enable me to consolidate or unify my OS environment?

Consumer vs Enterprise

USER VS IT CONTROLLED OS UPDATES

Consumer experience is about end-user convenience and control. In contrast the enterprise experience is about maximising productivity and enabling IT control. In the consumer model, OS updates are pushed to end users, bypassing IT. As updates are pushed out, end-users are given the authority / option to either update or ignore.

In several instances customers have attempted to block updates to their associate's devices by proxy URL filters. Unfortunately, download URL's were added and associates still managed to update their devices. The updates created application incompatibilities and / or a fragmented OS environment. Unfortunately, once the updates were loaded there was no way to rollback the OS.

The enterprise paradigm is quite different. Customers obtain updates from Zebra. Updates are loaded into an MDM where IT has complete control. IT determines when (often during off hours to reduce network loading during peak times) and which devices receive updates (e.g. rolling out incrementally to select facilities to reduce catastrophic failures). Because IT has the ability to perform "unattended updates", the transaction is independent and transparent to the end-user. Of course IT has the ability to push down either a newer release or revert back to a past release in the event an issue has arisen.

WI-FI PERFORMANCE

Mission Critical or Basic Connectivity

Wi-Fi performance represents a clear distinction between consumer and enterprise offerings. Consumer devices typically operate in sparsely populated AP environments, thus AP roaming efficiency is typically not a significant consideration. Poor roaming can result in significant variance in latency which can greatly impact voice and application response times, thereby degrading employee productivity.

Consumer vendors often tradeoff Wi-Fi connectivity for reduced cost and size. For example, Zebra devices typically provision with switched diversity antennas. Using 2 antennas instead of 1, impacts size and cost but provides robust Wi-Fi connectivity by transparently switching to the optimum antenna. This can eliminate what is called "phantom" effects which degrades connectivity based on hand or head placement relative to the device (which has been an issue with past Apple devices on the cellular network). In addition diversity antennas mitigate the impact of RF reflections (i.e. multipath) which creates wide fluctuations in connectivity and are pervasive in indoor enterprise environments.

In addition, as Wi-Fi networks become increasingly congested and interference more prevalent in the 2.4GHz band, the need for robust 5Ghz becomes increasingly important. For their Handheld devices Apple did not introduce 5GHz support until Gen 5 devices. In contrast to consumers, many enterprises were already using 5GHz for added capacity and to avert interference in the 2.4GHz band. However 5GHz performance can vary. As stated in a Gartner study in their evaluation of Apple iPads, "at 5Ghz, the IT organisation will need 300% more access points" (i.e. due to poor performance). This report is available for purchase from Gartner.

SCREEN SIZE

Improving Productivity

Enterprise customers are demanding increased screen size (while still balancing pocketability). One customer reported that they have been able to flatten their UI from 6 levels deep to a 2 levels based on the larger touch screen. This resulted in increased employee productivity. The larger screens have also enabled the use of portrait and landscape operation.

As Apple migrated from their 4th gen products to their 5th gen they changed screen size and aspect ratio. The newer screens are 4.0" with a 16:9 aspect ratio. In contrast the MC40 has a 4.3" display. At first glance the difference (4.0" to 4.3") sounds negligible; however, one must consider that the screen area is an exponential function of the diagonal. Thus, the MC40 has 19.3% more screen area than the Apple gen 5 devices. Furthermore based on enterprise customer feedback, Zebra released a 4.7" product in 2014 which has 38.1% more area than the Apple gen 5 products.

DEVICE VOLUME
2 Piece Sleds vs Integrated

Consumer devices with no peripheral add-ons are typically smaller and lighter than fully integrated enterprise solutions. However, when outfitted with a sled to add either payment functionality, supplemental battery capacity, and / or imaging for barcode reading, the consumer 2 piece solution often becomes larger than the enterprise integrated configuration.

For example, an iPod Touch Gen4 is a very compact ~47mm3 in volume. When fitted with an Infinite Peripheral sled to add barcode scanning and a battery capacity comparable to that of the MC40, the volume of this 2 piece solution rises to 199 mm3. This is larger than the MC40 volume of 173 mm3. In addition, the screen size of the iPod (gen 4) based solution is 3661 mm2 while the MC40 screen is 5264 mm2 (43% more screen area).

In short, with comparable functionality, the MC40 was 13.1% smaller in volume and provided 43% more screen area.

SLED SOLUTION
Drop Survivability

Enterprise devices are often categorised as “durable” or “rugged.” Enterprise durable devices are expected to be fully operational after 26 drops (6 side drops, 8 corner drops, 12 edge drops) from 4 foot to plywood. Zebra tested one well known sled solution (providing barcode scanning and additional battery) using the 26 drop test. The solution (sled & iPod) experienced 6 hard failures including; 1). a piece of the left latch broke off, 2). both volume trigger buttons (on the sled) fail to change the volume, 3). speakers fail to output any sound Scanners fail to function, 4). the unit fails to properly charge, 5). a piece of the LED lightpipe, on the bottom of the device, popped out, 6). a rattling noise can be heard towards the top of the device. The unit also exhibited 3 soft failures (failed to work but functionality restored after a reboot).

SLED SOLUTION
Switch and Contact Ratings

Generally consumer devices to not specify, and it is difficult to determine, the switch and contact ratings for 2piece sled solutions. These are however high failure items in enterprise use cases. As an example, the MC40 power button is rated for 500,000 cycles, the scan / camera button for 1,000,000 cycles, and the battery insertion for 2000 cycles (6000 for the terminal).

SLED SOLUTION
Battery Architecture

Feedback has come back to Zebra that a number of sled designs isolate the main battery from the sled battery (i.e. they do not share power). Thus both the iPod battery and the sled battery must be charged to have a functional unit. There are several sleds in the market so customers should validate the battery operation of the solution being evaluated. Recognise that independent battery operation may create life cycle issues over time.

AUDIO ACOUSTICS
Sound Pressure Levels

Consumer devices strive to be extremely thin even if it means trading off key enterprise features. Increasingly enterprise customers are seeking a converged voice / data device. Indoor users are converging traditional push-to-talk devices with data collection devices. In all instances, enterprises seek a device that can be reliably heard by the associate in relatively high noise environments.

To achieve the desired form factor, consumer devices typically sacrifice audio sound pressure level (SPL) and frequency response. Zebra has found that many popular consumer devices are 9 to 20dB lower in SPL than Zebra enterprise devices. Although subjective and non-linear based on the absolute output, 9dB difference in SPL levels generally equates to a perception of 2x the volume.

SLED FUNCTIONAL GRANULARITY

Integrated Barcode Scanning

In many instances enterprise customers desire aggressive scanning on all devices, all the time, and MPoS on select devices and / or only during select times of the year. When considering sled options they are forced to consider either procuring 2 different sled configurations (one for scanning only and one for scanning & payment) or to provision 100% of their devices with the more expensive, larger, scanning / payment option. Most prefer to have scanning integrated into the device and have payment relegated to a sled.

EXPANSION SLOT

Enterprise customers often request removable storage for porting data, for data backup, and / or for memory expansions. Apple devices do not offer removable media (e.g. SD cards, flash drives...).

NFC SUPPORT

Specifically an Apple issue, Apple has repeatedly decided not to support NFC. Many enterprise customers seek NFC for reading location markers, peripheral pairing, asset tag reading, and access control.

LAUNCHER FLEXIBILITY

In the case of Apple users have no option to replace or modify the launcher.

LOSS RATES

Device Shrinkage / Theft

Aftermarket demand for consumer devices is extremely high, increasing the motivation for theft. For consumer devices without interchangeable batteries, customers often procure 2 sets of devices, while one is in-use, a second is in a charging cradle. Customers have reported that devices in the charging area frequently go missing.

TEMPERATURE

Operating and Storage

Consumer devices generally have very limited operating and storage temperature range. For example Apple devices have an operating temperature range from +32F to +95F. When the device over-heats it becomes dysfunctional posting an exclamation point with a message to let the device cool down. A number of customers have reported this failure in relatively benign environments. In contrast enterprise class devices such as the Zebra MC65 have an operating temperature of +14F to +122F (i.e. 45 degrees of additional range compared to Apple). One customer reported that they were forced to place devices in an on-premise cooler to restore operation. Another customer reported the over-heating condition in Texas in November during a direct-store-delivery trial.

It is important to note that this is an ambient temperature specification. Thus, when the device is placed inside a sled the heat from the sled and the lack of a good external thermal path can further degrade the upper temperature range.

Storage temperature has also been reported as an issue for Apple devices. According to one customer exposure to a storage temperature marginally beyond the maximum rating of the device caused permanent degradation of battery life. The storage temperature ratings for an Apple device is -4F to +113F, in contrast the Zebra MC65 storage temperature rating is -40F to +158F.

ENTERPRISE DEVICE LIFE CYCLES

Consumer devices must keep in step with the latest trends and fashion. The typical shelf life (the time something becomes unsuitable for sale) for a smart phone is 6 to 9 months. Apple devices generally churn about every 12 months. The extent to which consumer companies make legacy devices available after the initial release is not defined. Enterprise customers have are forced between a very expensive completely a rip-and-replace or an incremental rolling rotation which is logistically complex and creates a highly fragmented deployment.

In the consumer space, legacy accessory compatibility is considered, but is not typically a primary requirement. Within Apple, the introduction of the Lightning connector (replacing the 30 pin connector) and the form factor changes introduced in iPhone5 forced enterprise customers to rip-and-replace their sleds, charging bays, and other accessories to migrate to the new device.

Enterprise devices such as those from Zebra typically have a 3+3 (6 years) or 5+5 (10 year) life cycle. The first term represents device availability and the second device support. Thus for a 3+3 customers can buy the device for 3 years and get service for an additional 3 years (a total life cycle of 6 years).

MAINTAINING ENTERPRISE SECURITY AND PRIVACY

Apple and Google (via Google Mobile Services-GMS) leverage devices to promote and sell services. Such services typically mandate (e.g. via EULA) access to device data which may breach corporate privacy and security policies. As an example, IBM publicly announced that it has banned Siri[1]. As stated in the Siri EULA — "you agree and consent to Apple's and its subsidiaries' and agents' transmission, collection, maintenance, processing, and use of this information, including your voice input and User Data." Because such devices require cloud connectivity, customers have been forced to punch holes in their corporate firewalls. Zebra customers including several top 10 retailers have stated that they will not allow GMS devices on their corporate network because of such privacy concerns.

CONSUMER ROADMAPS

Shrouded In Secrecy

Roadmap Privacy and secrecy are paramount to consumer offerings, but in direct conflict with enterprise planning and service continuity. Apple prides itself on secrecy:

- "The lack of information keeps the public interest high as consumers speculate" – Regis McKenna, one of the original Apple marketing consultants
- "Without a firm roadmap to work from, many buyers shy away from purchasing Apple products" – Jeff Gamet, MAC Observer

APP STORE MALWARE

Device Lockdown (MAM — Mobile Application Management)

As stated by NIST Mobile security guidelines, security best practice is to deny public App store access. Of course for consumer devices such as Apple this represents a significant value proposition and cannot be disabled.

Though Android's Google Play store has had a high degree of malicious content, apps on Apple App store can also breach enterprise data. Though Apple screens applications, it allows apps to retrieve and upload sensitive device data.

Key resources readily accessible (i.e. vulnerable) via valid IOS applications include:

- Wireless Communications to other devices
- Address book — mailing addresses, contact notes...etc.
- Calendar
- Device's identifier (a proprietary ID issued to each device by Apple)
- Device phone number (can be disabled via a configuration change)
- Music / video files and its photo gallery
- Safari search history
- Device's auto-completion history
- Recently viewed items in YouTube
- Wi-Fi connection logs
- Microphone and video camera

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

REMOVAL OF UNWANTED SERVICES

Given vulnerabilities introduced from public app stores, a number of customers attempted to remove the Apple App store from their IOS devices and reported “it keeps coming back.”

MOBILE APPLICATION MANAGEMENT (MAM) — INABILITY TO WHITE LIST

Corporate Liable Devices (CLD’s) are commonly locked down with respect to the applications allowed to be loaded and executed. Customers have expressed frustration in the inability to “White-List” (a list of allowed applications) consumer devices such as those running Apple / IOS (white-listing is a standard Androd / Mx feature).

MINDSHARE

“Pick a Partner” Not a Device”

In Q3 ’13 Apple sold 33.8M iPhones and Samsung sold 88.4M smartphones. That’s annualised rates of 135.2M and 353.6M units respectively. Thus, Samsung ships almost 1M units for every day of the year. A 10K unit enterprise rollout therefore represents only about 10% of a single day’s shipments. In contrast enterprise companies generally ship under 1.5M units / year. Thus a 10K unit opportunity represents a significant opportunity and warrants significant mindshare.

As one Zebra customer stated, when we picked a consumer offering we picked a device, not a partner. This mimics the sentiments recently expressed in a WSJ article[3].

LOGISTICS OVERHEAD

Distribution Certificate Updates

To distribute Apple applications, you must sign up under the Apple Enterprise developer program (enterprise certificate which lasts 3 yrs) and obtain a distribution certificate. Applications are then deployed, however, once the distribution certificate expires (1 year), you must rebuild your applications with a renewed certificate and then redeploy. As reported by several enterprise customers, the installed apps simply fails to run (may run for several days until the certificate is invalidated against Apple OCSP server).

REMOTE REBOOT

No matter how many precautions are taken devices sometimes require a reboot. Programmatic rebooting of the device requires API access not often available in consumer devices (e.g. Apple IOS). In contrast Zebra Android / Mx makes APIs available for trusted / signed applications to programmatically reboot the device (typically done remotely via MDM).

BATTERY MANAGEMENT

Maintaining Up-Time

Enterprise use cases often place considerable stress on battery life (both short & long term). In many instances consumer devices do not have the ability to replace batteries (e.g. Apple). In such instances Enterprise customers are forced to purchase 2 devices instead of one device and a replacement battery. In some scenarios the battery is replaceable, but the mechanical latching mechanism is not designed for repeated cycling and often fails over time.

“Designer Dustin Curtis reports that he did a quick survey of 15 developers of popular iOS apps, and ‘13 of them told me they have a contacts database with millions of records. One company’s database has Mark Zuckerberg’s cellphone number, Larry Ellison’s home phone number, and Bill Gates’ cellphone number.’”[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/

DEVICE ACCESS

E.G. Device Remote Control

The Apple IOS platform by design is relatively closed. Though this limits exposure to malicious content, it also limits the ability of enterprise developers to add advanced features. E.g., A commonly requested enterprise feature is to enable IT to remotely take control of the user's device. This is commonly used for training purposes and for diagnostics. To achieve this functionality, a trusted application must be granted access to the display buffer which is not made available on Apple platforms. In contrast, solutions such as Zebra's Android / Mx allow trusted applications (signed accordingly) to access resources like the frame buffer.

In short the Android signing process enables trusted, signed / authenticated applications the necessary level of access to enable enterprise features.

ULTRA-HIGH RESOLUTION

Balancing Enterprise Value

Consumer devices are migrating to ultra-high resolution displays. For example Apple from iPad2 to iPad New went from 1024x768 to 2048x1536. It has been reported that this transition required 2x more LEDs for backlighting and drove a +68% increase in the iPad New battery. As found in one study[4], the power efficiency of the display was significantly reduced (i.e. 2.5x the amount of power for the same brightness). Furthermore applications attempting to take advantage of the ultra-high resolution grew in size (e.g. Bjango went from 18.3MB to 35MB). Pushing larger payloads can increase cost when using a carrier with a tiered data pricing model.

Though high resolution is important to enterprise customers, extremes driven by consumer devices trading off battery life and / or weight are not necessarily beneficial.

FILE MANAGEMENT

Enterprise IT managers often desire the ability to view and manage files and folders within a device. Unfortunately the Apple IOS file system is not open. Though third party applications exist they are limited in their effectiveness due to the IOS architecture.

ENCRYPTION

Tradeoff Is File Size Optimisation

The efficiency of encryption implementation can vary depending on the target goal. Apple and Samsung implement hardware based encryption. Zebra testing has shown that for very large files (i.e. ~128MB, such as multimedia files) the Apple hardware encryption is effective. However, for small files (1KB) Zebra tests showed that the Zebra encryption implementation was 306% faster. The presumption is that the hardware crypto requires initialisation and setup which is amortised out for large files but impacts small files. Though hardware encryption may be very effective for large multimedia filed (e.g. DRM on movies) it may not be optimum for the smaller files often utilised in enterprise applications.

CENTRALISED STORAGE

In IOS, apps are universes among themselves and maintain their own storage that can only be accessed by that individual app. This complicates sharing large data structures (apps generally required to make another copy). When apps share data, the profile (e.g. encryption) of the original data structure may not be maintained in the copied structure, thus violating security policies.

Enterprise customers often request removable storage for porting data, for data backup, and / or for memory expansion. Apple devices do not support / offer removable media (e.g. SD cards, flash drives...).

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

MLC FLASH MEMORY MAY CORRUPT OVER PROLONGED USAGE

Flash memory is generally configured either as multi-level-cell (MCL) or single-level-cell (SLC). MLC configurations generally provide 2x the capacity of comparable SLC, but may cause data corrupt over time. After repeated use ("wear") the floating gate voltage levels representing bits of information in the MLC vary and bits are read in error.

Due to the relatively short life cycles and the relatively (compared to enterprise) benign usage, consumer devices and some enterprise devices use MLC Flash memory. Customers should validate their use case model / life cycle to determine the optimal flash configuration.

INABILITY TO LOCK CONFIGURATION PROFILES VIA MDM

Apple devices can be configured using "configuration profiles (CP)." Configuration profiles are XML files as specified by Apple. When an IT administrator configures a device with a CP, the CP can either be; open (readily modified), modified only with a passcode, or locked (any modifications will cause the device to be completely wiped).

When using profiles generated by an MDM there is no equivalent means to lock the CP. Thus the device profiles from an MDM can be readily changed or deleted by an end-user.

"ONE OS FROM WAREHOUSE TO STORE FLOOR" — NOT LIKELY WITH CONSUMER OFFERINGS

A top tier retailer (among others) has stated "we want one operating system from the warehouses to the store floor." Warehouses typically require very application specific devices, not likely to come from Apple. In contrast, Zebra (and we believe the broader industry) will be offering Android solutions from the warehouse, to the back-room, to the store floor, to a field associate.

CHOICE AND SELECTION

The Value of Competition

Pertaining primarily to Apple, Apple has a sole-source portfolio consisting of three basic devices; iPod, iPhone, and iPad. There are no application specific devices; all purposing is done through sleds. In contrast as of March 2013, there were well over 48 Android device manufacturers and over 550 devices available. This includes enterprise (e.g. Zebra, Honeywell, Bluebird…) and consumer device manufacturers. This diverse landscape provides enterprises more competitive pricing and the full benefits of multi-sourcing (e.g. reduced risk).

LIMITED API ACCESS

Enabling Enterprise Access

For Apple IOS & WP8, API's are locked down so as to minimise the attack surface available to malicious applications. Although potentially beneficial for consumers downloading unknown applications from unknown sources, this locked down approach significantly constraints features within enterprise, trusted applications (e.g. many enterprise customers desire detailed wireless controls, or access to hardware peripherals).

KEYCHAIN VULNERABILITY

Fraunhofer researchers have published a significant vulnerability in IOS. Many passwords (VPN access, Exchange Active Sync access password, Wi-Fi password, voicemail) in IOS are stored in the IOS keychain. This keychain in IOS is encrypted with "material" (data) stored locally on the device. Thus a hacker can extract the material from the device and decrypt the keychain…making stored passwords easily accessible. Note: that an update of this analysis is still pending for the latest release of IOS7.[5]

SIRI SECURITY VULNERABILITIES

Siri is a natural language voice recognition application introduced in iPhone4S. A large part of Siri's value is the ability to enable users rapid natural language queries. In a standard

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

configuration it is activated through a simple button press outside of the device lock. Thus if the device is lost or stolen, the bearer of the device can instantly get access to emails, contacts, text messages. Although Siri can be repositioned behind the lock firewall this would significantly diminish its value.

CONSUMER CAMERAS FOR BARCODE CAPTURE

Zebra generally defines two classes of imaging subsystems; “Camera” & “Imager.” As the name implies, the “Camera” is a multipurpose system typical of a consumer digital camera. Camera systems are typically; chromatic (color), auto-focus, high pixel count, wide angle of view, and excludes any form of aiming mechanism other than the viewfinder. Furthermore cameras generally shoot from the rear of the device. In contrast an “Imager” is generally monochromatic, fixed focus, lower pixel count with larger pixel apertures, a global shutter, a narrower angle-of-view, and inclusive of an aiming mechanism / pattern. Imagers are generally located in the front of the device (aka. a “front-shooter”).

Comparably important to a robust barcode capture system are the signal processing algorithms to acquire and decode barcodes within the image. Apple devices leveraging the Camera for barcode decode frequently use Red Laser decode software. Empirical testing of the Red Laser software has shown; frequent misdecodes, limited symbology support, and issues decoding corrupt or degraded barcodes.

For barcode reading applications, the imager subsystem has a longer life cycle, increased sensitivity, improved acquisition (aimer), and better immunity to hand jitter.

WI-FI FIPS ENCRYPTION

Government, healthcare, and some retailer (those with pharma and/or PCI for MPOS) customers are asking that the device’s cryptographic modules (i.e. those used for encryption/decryption) be certified to FIPS 140-2 Level 1. This level of FIPS assures best commercial practice design. FIPs certified cryptographic modules are generally available for enterprise and consumer devices. However, these modules do not typically apply to the Wi-Fi link cryptography (i.e. only for application use). Zebra has in the past offered FIPs on Microsoft based Wi-Fi products and in 2014 Zebra started offering FIPs on Wi-Fi for a number of our Android products.

For more information, visit www.zebra.com/mobilecomputers

NA and Corporate Headquarters
+1 800 423 0442
inquiry4@zebra.com

Asia-Pacific Headquarters
+65 6858 0722
contact.apac@zebra.com

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

Latin America Headquarters
+1 847 955 2283
la.contactme@zebra.com