



ZEBRA



Comparação entre Dispositivos para Consumidores e Empresariais

Visão geral

Este artigo apresenta um breve relatório executivo (dados de backup disponíveis mediante solicitação) de questões apontadas por clientes que tentam usar dispositivos de consumo em aplicações empresariais. Apesar de não especificar nenhum fornecedor de produtos de consumo, muitas das declarações são referentes à Apple, uma vez que ela tem um modelo muito único de plataforma / sistema operacional. De nenhuma maneira este documento deve ser visto como uma reprovação de dispositivos de consumo. O documento foi concebido para trazer uma “conscientização” dos compromissos feitos por fabricantes de dispositivos tanto empresariais quanto consumidores.

Aqueles que consideram dispositivos de consumo em aplicações empresariais devem considerar o seguinte:

- A minha solução será segura e manterá a minha privacidade de dados?
- Ela vai realisticamente sobreviver ao desgaste de um caso de uso empresarial?
- A solução (fornecedores, dispositivo, acessórios) poderá atender minhas necessidades de ciclo de vida?
- Estou permitindo que o TI gerencie / administre o portfólio de dispositivos de forma adequada?
- Eu tenho o mindshare do fornecedor, de modo a me apoiar adequadamente quando as coisas não saem como planejado?
- Estou confiante de que a solução será confiável o suficiente de modo a não afetar a produtividade dos funcionários ou a experiência dos clientes?
- Eu realmente examinei as questões que acompanham uma solução multi-peça?
- Será que a solução realmente atende aos requisitos funcionais atuais e futuros (desempenho sem fio, leitura de códigos de barras, áudio, temperatura, etc.)?
- Eu considere questões secundárias, como roubo do dispositivo?
- O meu fornecedor me permitirá planejar com antecedência? (por exemplo, visibilidade do plano de ação)
- Meus desenvolvedores e terceiros de ISV possuem acesso de interfaces de programação de aplicativo (API)?
- Meu plano me permitirá consolidar ou unificar o meu ambiente de sistema operacional?

Comparação entre Dispositivos para Consumidores e Empresariais

ATUALIZAÇÕES DE SISTEMA OPERACIONAL CONTROLADAS PELO TI VS. USUÁRIO

A experiência do consumidor se trata da conveniência e controle do usuário final. Em contraste, a experiência empresarial se trata de como maximizar a produtividade e permitir o controle do TI. No modelo de consumo, atualizações do sistema operacional são de responsabilidade dos usuários finais, contornando o TI. Como as atualizações são empurradas, os usuários finais têm a autoridade / opção de atualizar ou ignorar.

Em vários casos, os clientes têm tentado bloquear atualizações dos dispositivos de seus funcionários por filtros de proxy de URL. Infelizmente, foram adicionados URLs de download e os funcionários ainda conseguiam atualizar seus dispositivos. As atualizações criaram incompatibilidades de aplicativos e/ou um ambiente fragmentado de sistema operacional. Infelizmente, uma vez que as atualizações eram carregadas, não havia nenhuma maneira de reverter o sistema operacional.

O paradigma empresarial é bastante diferente. Os clientes obtêm as atualizações da Zebra. As atualizações são carregadas em um MDM onde o TI tem o controle completo. O TI determina quando (muitas vezes fora do horário de trabalho para reduzir a carga da rede durante o horário de pico) e quais dispositivos recebem atualizações (por exemplo, lançando de forma incremental para instalações selecionadas para reduzir falhas catastróficas). Uma vez que o TI tem a capacidade de executar “atualizações automáticas”, a transação é independente e transparente para o usuário final. E, obviamente, o TI tem a capacidade de derrubar uma versão mais recente ou reverter para um release antigo caso surja algum problema.

DESEMPENHO DO WI-FI

Missão Crítica ou Conectividade Básica

O desempenho do Wi-Fi representa uma clara distinção entre as ofertas de consumo e empresariais. Dispositivos de consumo normalmente operam em ambientes AP escassamente povoados, portanto, a eficiência de roaming do AP normalmente não é uma consideração importante. Um roaming fraco pode resultar em variação significativa na latência, que pode ter grande impacto nos tempos de resposta dos aplicativos e de voz, degradando, assim, a

produtividade dos funcionários.

Fornecedores de dispositivos de consumo muitas vezes trocam a conectividade Wi-Fi para reduzir o custo e o tamanho. Por exemplo, os dispositivos da Zebra normalmente dispõem de antenas de diversidade comutada. Usar 2 antenas em vez de 1 afeta o tamanho e os custos, mas oferece conectividade Wi-Fi robusta ao trocar para a antena ideal. Isto pode eliminar o chamado efeito “fantasma” que degrada a conectividade com base no posicionamento na mão ou na cabeça relativo ao dispositivo (o que tem sido um problema com os dispositivos antigos da Apple na rede celular). Além disso, antenas de diversidade mitigam o impacto das reflexões RF (isto é, multipath), que criam grandes flutuações na conectividade e estão presentes em ambientes corporativos internos.

Além disso, como redes Wi-Fi se tornam cada vez mais congestionadas e interferências mais prevalentes na banda de 2,4 GHz, a necessidade de 5 GHz robusto se torna cada vez mais importante. Para os seus dispositivos portáteis, a Apple não introduziu suporte 5 GHz até dispositivos de 5ª geração. Em contraste com os consumidores, muitas empresas já estavam usando 5 GHz para capacidade adicional e para evitar interferência na banda de 2,4 GHz.

No entanto, o desempenho 5 GHz pode variar. Conforme afirmado em um estudo do Gartner em sua avaliação dos iPads da Apple, “em 5 GHz, a organização do TI terá 300% mais pontos de acesso” (isto é, devido ao mau desempenho). O relatório está disponível para compra na Gartner.

TAMANHO DA TELA

Aumento de Produtividade

Os clientes empresariais estão exigindo aumento do tamanho da tela (mas ainda em tamanho de bolso). Um cliente informou que conseguiu achatar sua UI de 6 níveis de profundidade para 2 níveis com base na maior tela sensível ao toque. Isso resultou em maior produtividade do funcionário. As telas maiores também possibilitaram o uso de operação retrato e paisagem.

Conforme a Apple migrou seus produtos da 4ª geração para a 5ª geração, mudaram o tamanho e o formato da tela. As novas telas são de 4,00" com formato 16:9. Em contraste, o MC40 possui uma tela de 4,3". À primeira vista, a diferença (de 4,0" para 4,3") soa insignificante; no entanto, é preciso considerar que a área da tela é uma função exponencial da diagonal. Assim, o MC40 tem 19,3% mais área de tela do que os dispositivos da 5ª geração da Apple. Além disso, com base no feedback de clientes empresariais, a Zebra lançou um produto de 4,7" em 2014, que tem 38,1% mais área do que os produtos da 5ª geração da Apple.

VOLUME DO DISPOSITIVO

Sleds de 2 Peças vs. Integrada

Dispositivos de consumo sem complementos periféricos são geralmente menores e mais leves do que as soluções empresariais totalmente integradas. No entanto, quando equipado com um sled para adicionar funcionalidades de pagamento, capacidade suplementar de bateria, e/ou imagem para leitura de códigos de barras, a solução de consumo de 2 peças muitas vezes se torna maior do que a configuração integrada empresarial.

Por exemplo, um iPod Touch de 4ª geração é muito compacto em volume, com ~47mm³. Quando equipado com um sled periférico Infinite para adicionar leitura de códigos de barras e uma capacidade de bateria comparável à do MC40, o volume desta solução de 2 peças sobe para 199 mm³. Isso é maior do que o volume de 173 mm³ do MC40. Além disso, o tamanho da tela do iPod (geração 4) é 3661 mm², enquanto a tela do MC40 é 5264 mm² (43% mais área de tela).

Em suma, com uma funcionalidade comparável, o MC40 foi 13,1% menor em volume e ofereceu 43% mais área de tela.

SOLUÇÃO DE SLED

Sobrevivência a Quedas

Dispositivos empresariais são frequentemente classificados como "duráveis" e "robustos". Espera-se que dispositivos empresariais duráveis continuem totalmente operacionais depois de 26 quedas (6 quedas de lado, 8 quedas de canto, 12 quedas de borda) de 4 pés em madeira compensada. A Zebra testou uma solução de sled bem conhecida (fornecendo leitura de códigos de barras e bateria adicional), utilizando o teste de 26 quedas.

A solução (sled e iPod) sofreu 6 falhas graves, incluindo:

- 1). uma peça da trava esquerda quebrou, 2). os dois botões de volume (no sled) não alteraram o volume, 3). alto-falantes não emitem quaisquer sons e Scanners não funcionam, 4). a unidade não carrega corretamente, 5). um pedaço do tubo de luz LED, na parte inferior do dispositivo, caiu, 6). um ruído pode ser ouvido no topo do dispositivo.

A unidade também exibiu 3 falhas leves (não funcionou, mas a funcionalidade foi restaurada após uma reinicialização).

SOLUÇÃO DE SLED

Classificações de Contato e Comutação

Geralmente, dispositivos de consumo não especificam, e é difícil de se determinar, as classificações de contato e comutação para soluções de sled de 2 peças. Porém, eles são itens de falhas graves em casos de uso empresarial. Como exemplo, o botão de energia do MC40 é classificado para 500.000 ciclos, o botão de leitura/câmera para 1.000.000 ciclos e a inserção da bateria para 2000 ciclos (6000 para o terminal).

SOLUÇÃO DE SLED

Arquitetura da Bateria

A Zebra recebeu feedback de que uma série de designs de sled isolam a bateria principal da bateria da armação (ou seja, eles não dividem a energia). Portanto, tanto a bateria do iPod quanto a bateria do sled devem ser carregadas para se conseguir uma unidade funcional. Existem vários sleds no mercado, então os clientes devem validar a operação da bateria da solução que está sendo avaliada. Lembre-se que a operação independente da bateria pode criar problemas no ciclo de vida ao longo do tempo.

ACÚSTICA DE ÁUDIO

Nível de Pressão Sonora

Dispositivos de consumo buscam ser extremamente finos, mesmo que isso signifique abrir mão de características empresariais fundamentais. Cada vez mais os clientes empresariais procuram um dispositivo que combine voz e dados.

Usuários de ambientes internos estão convergindo dispositivos push-to-talk tradicionais com dispositivos de coleta de dados.

Em todos os casos, as empresas buscam um dispositivo que possa ser confiavelmente ouvido pelo funcionário em ambientes relativamente elevados de ruído.

Para alcançar o fator de forma desejado, dispositivos de consumo normalmente sacrificam o nível de pressão sonora (SPL) do áudio e a resposta de frequência. A Zebra descobriu que muitos dispositivos de consumo populares são de 9 a 20 dB menores em SPL do que os dispositivos empresariais da Zebra. Embora subjetivo e baseado de forma não linear na saída absoluta, a diferença de 9 dB nos níveis de SPL geralmente equivale a uma percepção de 2x o volume.

GRANULARIDADE FUNCIONAL DO SLED

Leitura Integrada de Códigos de Barras

Em muitos casos, os clientes empresariais desejam leitura agressiva em todos os dispositivos, o tempo todo, e MpoS em dispositivos selecionados e/ou apenas durante determinadas épocas do ano. Ao considerar as opções de sled, eles são forçados a considerar a aquisição de 2 configurações diferentes de sled (um apenas para leitura e um para leitura e pagamento) ou equipar 100% de seus dispositivos com a opção mais cara e maior de leitura / pagamento. A maioria prefere ter leitura integrada no dispositivo e deixar o pagamento por conta do sled.

SLOT DE EXPANSÃO

Os clientes corporativos muitas vezes solicitam armazenamento removível para portar dados, para backup de dados e/ou para expansões de memória. Os dispositivos da Apple não oferecem mídia removível (por exemplo, cartões SD, flash drives, etc.).

SUPORTE NFC

Especificamente um problema da Apple, a Apple decidiu repetidamente não apoiar NFC. Muitos clientes empresariais procuram NFC para ler marcadores de localização, conexão periférica, leitura da etiquetas de inventário e controle de acesso.

FLEXIBILIDADE DE INICIADOR

No caso da Apple, os usuários não têm a opção de substituir ou modificar o iniciador.

TAXAS DE PERDA

Redução / Roubo de Dispositivos

A demanda de reposição para dispositivos de consumo é extremamente alta, aumentando a motivação para o roubo. Para dispositivos de consumo sem baterias intercambiáveis, os clientes muitas vezes adquirem 2 conjuntos de dispositivos, enquanto um está em uso, um segundo está em uma base de carregamento. Os clientes relataram que os dispositivos na área de carregamento frequentemente somem.

TEMPERATURA

Operação e Armazenamento

Dispositivos de consumo geralmente têm uma faixa de temperatura de operação e armazenamento muito limitada.

Por exemplo, dispositivos da Apple têm uma faixa de temperatura de +32F a +95F. Quando o dispositivo superaquece, torna-se disfuncional, aparecendo ponto de exclamação com uma mensagem para deixar o dispositivo esfriar. Diversos clientes relataram essa falha em ambientes relativamente benignos. Em contraste, dispositivos de classe empresarial, tais como o MC65 da Zebra, têm uma faixa de temperatura operacional de +14F a +122F (ou seja, 45 graus de faixa adicional em comparação com a Apple). Um cliente informou que foi obrigado a colocar os dispositivos em um refrigerador no local para restaurar a operação. Outro cliente relatou a condição de superaquecimento no Texas em novembro durante um teste de entrega direta à loja.

É importante observar que essa é uma especificação de temperatura ambiente. Assim, quando o dispositivo é colocado dentro de um sled, o calor do sled e a falta de um bom caminho térmico externo pode degradar ainda mais a faixa de temperatura mais alta.

A temperatura de armazenamento também foi relatada como um problema para os dispositivos da Apple. De acordo com um cliente, uma exposição a uma temperatura de armazenamento marginalmente superior à classificação máxima do dispositivo causou degradação permanente da vida da bateria. As classificações de temperatura de armazenamento para um dispositivo Apple são de -4F a +113F. Em contraste, a classificação de temperatura de armazenamento do MC65 da Zebra é de -40F a +158F.

CICLOS DE VIDA DE DISPOSITIVOS EMPRESARIAIS

Dispositivos de consumo devem se manter em sintonia com as últimas tendências e modas. A vida útil (o tempo até algo se tornar impróprio para venda) típica de um smartphone é de 6 a 9 meses. Dispositivos da Apple geralmente são renovados a cada 12 meses.

A medida em que as empresas de dispositivos de consumo tornam os dispositivos existentes disponíveis após o lançamento inicial não está definida. Os clientes corporativos são forçados a escolher entre um dispositivo muito caro de substituir ou uma rotação incremental que é logisticamente complexa e cria uma implementação altamente fragmentada.

No espaço do consumidor, a compatibilidade de acessórios existentes é considerada, mas normalmente não é uma exigência principal. Dentro da Apple, a introdução do conector Lightning (substituindo o conector de 30 pinos) e as mudanças de fator de forma introduzidas no iPhone 5 forçaram clientes corporativos a substituir seus sleds, estações de carregamento e outros acessórios para migrar para o novo dispositivo.

Dispositivos empresariais, tais como os da Zebra, normalmente possuem um ciclo de vida de 3+3 (6 anos) ou 5+5 (10 anos). O primeiro período representa disponibilidade do dispositivo e o segundo representa suporte de dispositivo. Portanto, para um período de 3+3, os clientes podem comprar o dispositivo por 3 anos e obter serviço por um período adicional de 3 anos (um ciclo de vida total de 6 anos).

MANUTENÇÃO DA SEGURANÇA E PRIVACIDADE EMPRESARIAL

Apple e Google (via Google Mobile Services - GMS) usam os dispositivos para promover e vender serviços. Esses serviços normalmente requerem (por exemplo, através de EULA) acesso aos dados do dispositivo, o que pode violar as políticas de privacidade e segurança corporativa. Como um exemplo, a IBM anunciou publicamente que baniu a Siri¹. Como se afirma no EULA da Siri - "você concorda e consente que a Apple e suas subsidiárias e agentes de transmissão, coleta, manutenção e processamento utilizem a informação, incluindo sua entrada de voz e dados do usuário". Uma vez que tais dispositivos exigem conectividade em nuvem, os clientes têm sido forçados a abrir buracos em seus firewalls corporativos.

Os clientes da Zebra, incluindo vários varejistas, declararam que não permitirão dispositivos GMS na sua rede corporativa por causa de tais preocupações com a privacidade.

PLANOS DE AÇÃO DE CONSUMO Envolto em Sigilo

Privacidade e sigilo do plano de ação são fundamentais para ofertas ao consumidor, mas em conflito direto com o planejamento empresarial e a continuidade de serviço. A Apple se orgulha do sigilo:

- "A falta de informações mantém o interesse público alto conforme os consumidores especulam"- Regis McKenna, um dos consultores de marketing originais da Apple.
- "Sem um plano de ação firme para desenvolver, muitos compradores evitam a compra de produtos da Apple" - Jeff Gamet, Observador MAC

MALWARE NA LOJA DE APLICATIVOS Bloqueio do Dispositivo (MAM - Gerenciamento de Aplicativo Móvel)

Conforme afirmado por diretrizes de segurança móvel do NIST, a prática de segurança recomendada é negar o acesso público à App Store. É claro que para dispositivos de consumo, como os da Apple, isso representa uma proposta de valor significativo e não pode ser desativada.

Embora o Google Play do Android tenha tido um alto grau de conteúdo malicioso, aplicativos no App Store da Apple também podem violar dados da empresa. Embora a Apple filtre aplicativos, ela permite que aplicativos recuperem e façam upload de dados confidenciais do dispositivo.

Recursos essenciais facilmente acessíveis (isto é, vulneráveis) por meio de aplicativos IOS válidos incluem:

- Comunicações sem fio com outros dispositivos
- Agenda de endereços - endereços de correspondência, notas de contato, etc.
- Calendário
- Identificador do dispositivo (a identificação proprietária emitida para cada dispositivo pela Apple)
- O número de telefone do dispositivo (pode ser desabilitado mudando as configurações)
- Arquivos de música/vídeo e galeria de fotos
- Histórico de busca no Safari
- Histórico de autopreenchimento do dispositivo
- Últimos vídeos assistidos no YouTube
- Registros de conexão Wi-Fi
- Microfone e vídeo da câmera

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

REMOÇÃO DE SERVIÇOS INDESEJADOS

Dadas as vulnerabilidades introduzidas a partir de lojas de aplicativos públicos, uma série de clientes tentaram remover a App Store da Apple de seus dispositivos IOS e relataram que “ela continua voltando”.

GERENCIAMENTO DE APLICATIVO MÓVEL (MAM) - INCAPACIDADE DE INCLUIR NA LISTA DE PERMISSÕES

Dispositivos com plano corporativo (CLDs) são normalmente bloqueados com os aplicativos autorizados a serem carregados e executados. Os clientes têm expressado frustração na incapacidade de “incluir na lista de permissões” (lista de aplicativos permitidos) dispositivos de consumo, como os que executam Apple / IOS (inclusão na lista de permissões é um recurso padrão do Android / Mx).

MINDSHARE

“Escolha um Parceiro, Não um Dispositivo”

No terceiro trimestre de 2013, a Apple vendeu 33,8M de iPhones e a Samsung vendeu 88,4M de smartphones. Esses números resultam em taxas anualizadas de 135,2M e 353,6M unidades, respectivamente. Assim, a Samsung envia quase 1M de unidades a cada dia do ano. Portanto, uma distribuição de 10K unidades empresariais representa apenas cerca de 10% dos envios de um único dia.

Em contraste, empresas de dispositivos empresariais enviam, geralmente, um pouco menos de 1,5M unidades/ano. Assim, uma oportunidade de 10K unidades representa uma oportunidade significativa e garante mindshare significativo.

Como um cliente da Zebra afirmou, quando aceitamos uma oferta ao consumidor, escolhemos um dispositivo, não um parceiro. Isso reflete os sentimentos recentemente expressos em um artigo do WSJ³.

SOBRECARGA DE LOGÍSTICA

Atualizações de Certificados de Distribuição

Para distribuir aplicativos da Apple, você deve se inscrever no programa de desenvolvedores da Apple Enterprise (certificado corporativo com validade de 3 anos) e obter um certificado de distribuição. Os aplicativos são então instalados, no entanto, uma vez que o certificado de distribuição expira (1 ano), você tem de reconstruir seus aplicativos com um certificado renovado e, em seguida, reinstalar. Conforme relatado por vários clientes empresariais, os aplicativos instalados simplesmente não funcionam (podem ser executados por vários dias até que o certificado seja invalidado no servidor OCSP da Apple).

REINICIALIZAÇÃO REMOTA

Não importa quantas precauções são tomadas, os dispositivos às vezes requerem uma reinicialização.

A reinicialização programática do dispositivo requer acesso a API muitas vezes não disponível em dispositivos de consumo (por exemplo, o IOS da Apple). Em contraste, Android / Mx da Zebra disponibilizam APIs para aplicativos confiáveis / assinados para reiniciar programaticamente o dispositivo (normalmente feito remotamente via MDM).

GERENCIAMENTO DE BATERIA

MANUTENÇÃO DO TEMPO DE FUNCIONAMENTO

Casos de uso empresarial muitas vezes colocam uma pressão considerável sobre a vida da bateria (tanto em curto quanto em longo prazo).

Em muitos casos, dispositivos de consumo não têm a capacidade de substituir as baterias (por exemplo, Apple).

Em tais casos, clientes corporativos são forçados a comprar dois dispositivos em vez de um dispositivo e

“O designer Dustin Curtis relata que fez uma rápida pesquisa com 15 desenvolvedores de aplicativos iOS populares, e ‘13 deles me disseram que têm uma base de dados de contatos com milhões de registros. O banco de dados de uma empresa tem o número do celular do Mark Zuckerberg, o número do telefone residencial de Larry Ellison, e o número do celular do 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-still-lags-in-enterprise-support/>

uma bateria reserva. Em alguns cenários a bateria é substituível, mas o mecanismo de travamento mecânico não foi projetado para o ciclismo repetido e muitas vezes falha ao longo do tempo.

ACESSO AO DISPOSITIVO

Controle Remoto do Dispositivo

A plataforma IOS da Apple é relativamente fechada por predefinição. Embora isso limite a exposição a conteúdo malicioso, também limita a capacidade dos desenvolvedores corporativos de adicionarem recursos avançados. Por exemplo, uma característica empresarial comumente solicitada é habilitar o TI a controlar remotamente o dispositivo do usuário. Este recurso é comumente usado para fins de treinamento e diagnóstico. Para obter essa funcionalidade, deve-se conceder acesso de um aplicativo confiável ao buffer de exibição que não é disponibilizado em plataformas da Apple. Em contraste, soluções como o Android / Mx da Zebra permitem que aplicativos confiáveis (assinados em conformidade) para acessar recursos como o buffer de quadros.

Em suma, o processo de assinatura do Android concede a aplicativos confiáveis, assinados / autenticadas o nível necessário de acesso para habilitar os recursos empresariais.

ULTRA-ALTA RESOLUÇÃO

Equilibrando o Valor Empresarial

Dispositivos de consumo estão migrando para telas de ultra-alta resolução. Por exemplo, a Apple, do iPad2 para o iPad New, passou de 1024x768 para 2048x1536. Tem sido relatado que esta transição exigiu 2x mais LEDs para iluminação de fundo e impulsionou um aumento de +68% na bateria do iPad New. Como demonstrado em um estudo⁴, a floor

eficiência de energia da tela foi significativamente reduzida (ou seja, 2,5x a quantidade de energia para o mesmo brilho). Além disso, aplicativos que tentam tirar proveito da ultra-alta resolução cresceram em tamanho (por exemplo, Bjango passou de 18,3 MB para 35 MB). Cargas úteis maiores podem aumentar o custo quando se utiliza um transportador com um modelo de precificação de dados em camadas.

Embora a alta resolução seja importante para clientes corporativos, os extremos dos dispositivos de consumo, que abrem mão da vida e/ou do peso da bateria, não são necessariamente benéficos.

GERENCIAMENTO DE ARQUIVOS

Gerentes corporativos de TI muitas vezes desejam ter a capacidade de visualizar e gerenciar arquivos e pastas dentro de um dispositivo. Infelizmente, o sistema de arquivos do IOS da Apple não é aberto. Embora existam aplicativos de terceiros, eles são limitados em sua eficácia devido à arquitetura do IOS.

CRIPTOGRAFIA

Otimização do Tamanho dos Arquivos

A eficiência da execução de criptografia pode variar, dependendo do objetivo alvo. Apple e Samsung implementam criptografia baseada em hardware. Testes da Zebra mostraram que para arquivos muito grandes (ou seja, ~128 MB, como arquivos multimídia) a criptografia de hardware da Apple é eficaz. No entanto, para arquivos pequenos (1 KB), os testes da Zebra mostraram que a implementação de criptografia da Zebra foi 306% mais rápida. A suposição é que a criptografia de hardware requer inicialização e configuração, que são amortizadas para arquivos grandes, mas afetam arquivos pequenos. Embora a criptografia de hardware possa ser muito eficaz para grandes arquivos multimídia (por exemplo, DRM em filmes), pode não ser ideal para arquivos menores, muitas vezes utilizados em aplicações empresariais.

ARMAZENAMENTO CENTRALIZADO

No IOS, aplicativos são universos isolados e mantêm seu próprio armazenamento, que só pode ser acessado por aquele aplicativo individual. Isso complica o compartilhamento de estruturas de dados grandes (aplicativos geralmente necessários para fazer outra cópia). Quando os aplicativos compartilham dados, o perfil (por exemplo, a criptografia) da estrutura de dados original não pode ser mantido na estrutura copiada, violando, assim, as políticas de segurança.

Os clientes corporativos muitas vezes solicitam armazenamento removível para portar dados, para backup de dados e/ou para expansões de memória. Os dispositivos da Apple não oferecem/suportam mídia removível (por exemplo, cartões SD, flash drives, etc.).

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

MEMÓRIA FLASH MLC PODE SER CORROMPIDA COM USO PROLONGADO

A memória flash é geralmente configurada tanto como célula multinível (MCL) ou célula de nível único (SLC). As configurações MLC geralmente proporcionam 2x a capacidade de SLC comparável, mas podem causar corrupção dados ao longo do tempo. Após o uso repetido (“desgaste”) os níveis de tensão da porta flutuante que representam bits de informação na MLC variam, e os bits são lidos com erro.

Devido aos ciclos de vida relativamente curtos e ao uso relativamente (em comparação com o empresarial) benigno, dispositivos de consumo e alguns dispositivos empresariais usam memória MLC flash. Os clientes devem validar seu modelo de caso de uso / ciclo de vida para determinar a configuração flash ideal.

INCAPACIDADE DE BLOQUEAR OS PERFIS DE CONFIGURAÇÃO ATRAVÉS DE MDM

Os dispositivos da Apple podem ser configurados usando “perfis de configuração (CP)”. Os perfis de configuração são arquivos XML, conforme especificado pela Apple. Quando um administrador de TI configura um dispositivo com um CP, o CP pode ser: open (facilmente modificado), modificado apenas com uma senha, ou bloqueado (qualquer modificação fará com que o dispositivo seja completamente apagado).

Ao usar perfis gerados por um MDM, não há meios equivalentes para bloquear o CP. Assim, os perfis de dispositivos a partir de um MDM podem ser facilmente alterados ou excluídos por um usuário final.

“UM ÚNICO SISTEMA OPERACIONAL DESDE O ARMAZÉM ATÉ A ÁREA DE VENDAS” - NÃO É PROVÁVEL COM DISPOSITIVOS DE CONSUMO

Um varejista importante (dentre outros) declarou que “nós queremos um único sistema operacional desde os armazéns até a área de vendas”. Armazéns normalmente requerem dispositivos para aplicações muito específicas, que provavelmente não serão fornecidos pela Apple. Em contraste, a Zebra (e nós acreditamos que a indústria mais ampla) oferecerá soluções de Android para o armazém, a área administrativa, a área de vendas, um funcionário de campo.

ESCOLHA E SELEÇÃO

O Valor da Concorrência

A Apple tem um portfólio de fonte única que consiste de três dispositivos básicos: iPod, iPhone e iPad. Não há dispositivos para aplicações específicas; toda a especificação é feita através de sleds. Em contraste, a partir de março de 2013, havia mais de 48 fabricantes de dispositivos Android e mais de 550 dispositivos disponíveis. Isso inclui fabricantes de dispositivos de consumo e empresariais (por exemplo, Zebra, Honeywell, Bluebird, etc.). Esta paisagem diversificada oferece às empresas preços mais competitivos e benefícios de multi-sourcing (por exemplo, risco reduzido).

ACESSO LIMITADO A API

Habilitando Acesso Empresarial

Para o IOS da Apple e o WP8, APIs são bloqueadas de modo a minimizar a superfície de ataque disponível para aplicativos maliciosos. Embora potencialmente benéfico para os consumidores que baixam aplicativos desconhecidos de fontes desconhecidas, esta abordagem de bloqueio restringe de maneira significativa os recursos dentro dos aplicativos empresariais confiáveis (por exemplo, muitos clientes corporativos desejam controles sem fio detalhados, ou acesso aos periféricos de hardware).

VULNERABILIDADE DAS CHAVES

Pesquisadores da Fraunhofer publicaram uma vulnerabilidade significativa no IOS. Muitas senhas (acesso VPN, senha de acesso ao Exchange Active Sync, senha Wi-Fi, correio de voz) no IOS são armazenadas nas chaves do IOS. Estas chaves do IOS são criptografadas com “materiais” (dados) armazenados localmente no dispositivo. Portanto, um hacker pode extrair o material do dispositivo e descriptografar as chaves... tornando as senhas armazenadas facilmente acessíveis. Observação: uma atualização desta análise ainda está pendente para a versão mais recente do iOS7.⁵

VULNERABILIDADES NA SEGURANÇA DA SIRI

Siri é um aplicativo de reconhecimento de voz em linguagem natural introduzido no iPhone 4S. Uma grande parte do valor da Siri é a capacidade de permitir que os usuários façam consultas rápidas em linguagem natural.

⁵ “Fraunhofer researchers circumvent encryption devices iPhone”, Latest IT News, Feb 9, 2011

Em uma configuração padrão, ela é ativada através do simples pressionar de um botão fora do bloqueio do dispositivo. Assim, se o dispositivo for perdido ou roubado, o portador do dispositivo pode imediatamente ter acesso a e-mails, contatos, mensagens de texto. Embora a Siri possa ser reposicionada para dentro do firewall de bloqueio, isso reduziria significativamente o seu valor.

CÂMERAS DE CONSUMO PARA CAPTURAR CÓDIGOS DE BARRAS

A Zebra geralmente define duas classes de subsistemas de imagem: “Câmera” e “Gerador de Imagem”. Como o nome indica, a “Câmera” é um sistema multifuncional típico de uma câmera digital de consumo. Sistemas de câmera são tipicamente: cromático (colorido), focagem automática, alta contagem de pixels, amplo ângulo de visão, e excluem qualquer forma de mecanismo de direcionamento que não seja o viewfinder. Além disso, câmeras geralmente disparam a partir da parte traseira do dispositivo. Em contraste, um “Gerador de Imagem” é geralmente monocromático, de foco fixo, com menor contagem de pixels e maiores aberturas de pixels, um obturador global, um ângulo de visão mais estreito, e inclui um mecanismo / padrão de direcionamento. Geradores de imagem estão geralmente localizados na parte da frente do dispositivo (ou seja, “disparador frontal”).

Igualmente importante para um sistema robusto de captura de códigos de barras são os algoritmos de processamento de sinal para adquirir e decodificar códigos de barras dentro da imagem.

Os dispositivos da Apple que aproveitam a câmera para decodificação de códigos de barras frequentemente utilizam o software de decodificação Red Laser. Testes empíricos do software Red Laser mostraram: erros frequentes de decodificação, suporte limitado de simbologia e problemas de decodificação de códigos de barras corrompidos ou degradadas.

Para aplicativos de leitura de códigos de barras, o subsistema do gerador de imagens tem um ciclo de vida mais longo, maior sensibilidade, melhor aquisição (direcionamento) e melhor imunidade ao tremor da mão.

CRIPTOGRAFIA DE FIPS DO WI-FI

Clientes do governo, saúde e alguns varejistas (aqueles com a indústria farmacêutica e/ou PCI para MPOs) estão pedindo que os módulos de criptografia do dispositivo (ou seja, aqueles utilizados para encriptação/descriptação) sejam certificados para FIPS 140-2 Nível 1. Esse nível de FIPS garante a melhor prática comercial. Módulos criptográficos com FIPs certificados estão geralmente disponíveis para dispositivos empresariais e de consumo. No entanto, estes módulos normalmente não se aplicam à criptografia de link Wi-Fi (ou seja, apenas para uso do aplicativo). No passado, a Zebra ofereceu FIPs sobre produtos com Wi-Fi baseado em Microsoft e, em 2014, começou a oferecer FIPs sobre Wi-Fi para uma série de nossos produtos Android.

Para mais informações, visite www.zebra.com/mobilecomputers



Sede América Latina | +55 11 4130 8178 | la.contactme@zebra.com