CLASSIFICAÇÃO:			
X	**NÃO CLASSIFICADO**		NÃO CLASSIFICADO
	CLASSIFICADO		PRIVADO
	SECRETO		PARTICULAR
	ALTAMENTE SECRETO	**X**	**PÚBLICO**

FreeBSD Brasil LTDA.

Av. Getúlio Vargas, 54 – 3° andar, Funcionários – Belo Horizonte, MG

Patrick Tracanelli, Ger. de Consultoria – patrick@freebsdbrasil.com.br – Tel.: (31) 3516-0800

Termo de Confidencialidade

Documentação, Versões e Histórico.

Versão	Data	Autor(es)	Histórico
1.0	10/06/10	Patrick	Elaboração a pedido de Cliente.
1.1	11/06/10	Patrick	Revisão e liberação versão pública.

Sumário

1 - Apresentação

Afim de apoiar a decisão sobre adoção / padronização de dispositivos móveis do tipo smartphones em ambiente corporativo, a FreeBSD Brasil LTDA preparou o documento comparativo aqui disponível.

O objetivo desse estudo é avaliar as principais opções de smartphones no mercado hoje, como foco exclusivamente na disponibilidade de recursos de segurança. Os itens avaliados são os usualmente necessários para conformidade com PCSI (Política Corporativa de Segurança da Informação) fundada nos pilares da BS7799 / ISO-IEC 27000 e controles CobIT.

É importante notar que a avaliação é de disponibilidade de recursos apenas. A funcionalidade, eficiência ou garantias intrínsecas ao uso desses recursos não foram avaliadas. A avaliação final é meramente matemática. Para cada item avaliado, foram atribuídos 2 pontos para os recursos disponíveis, 1 ponto para os parcialmente disponíveis ou disponíveis com ressalvas e 0 pontos para os recursos indisponíveis.

1.1 - Dispositivos avaliados

Os dispositivos utilizados foram um BlackBerry 8320, versão de Software 5.0; iPhone 3GS versão de Software iPhoneOS 3.0; Nokia N900 versão de software Maemo 5/PR1.2; Nexus One versão de software Android v2.2.

2 – Tabela Comparativa de Recursos de Segurança

Descrição / Recurso	RIM BlackBerry	Apple iPhone	Nokia Maemo	Google Android
Provisionamento Padronizado / Automatizado	Disponível parcialmente por operadora através do recurso BIS. Disponível integralmente de forma corporativa via BES (BlackBerry Enterprise Server)	Disponível parcialmente através de rotina AppleScript em Mac OS X Server Leopard apenas.	Disponível extra-oficialmente em rotinas customizáveis Python em aplicação disponível no repositório extras.	Teoricamente possível por shell script e leitura de configurações em XML. Não há framework padronizado disponível.
Policy / Domínio	Disponível integralmente através do BES.	Disponível parcialmente (apenas 4 recursos: WiFi Join, Apple App Killswitch, Auto-lock, Password llock) com uso de Mac OS X Server Leopard.	Indisponível.	Indisponível.
Sincronização de Data/Hora	Sim, BES / Operadora, NTP	Sim, Mac OS X Server Leopard, NTP, Operadora.	Sim, OpenNTP, NTP, Samba, Operadora, OVI/Nokia. Incluindo balanceamento de todos eles.	Sim, AD, NTP, Operadora.
Criptografia Memória / Dados por Software	Sim, senha e PIN.	Oficialmente não. Disponível através de Software Adicional de terceiros (9,99 dólares Apple Store). Apenas senha.	Oficialmente não. Disponível em repositório padrão, PIN e senha.	Não oficialmente.
Criptografia Memória / Hardware	Sim, por padrão.	Não.	Sim, disponível no repositório extras-testing.	Não.
Controle de Recepção MMS.	Sim, BES.	Não.	Não por padrão. Parcial com solução de terceiros (extras-testing).	Não por padrão. Teoricamente disponível através de *hack* da comunidade.
Controle de Conexões.	Sim, USB, BlueTooth, Telefone, WiFi, GPS, GPRS, EDGE, 3G.	Apenas iTunes via Mac OS X Leopard Server.	Sim, por meio de aplicação em extras-testing. USB, BlueTooth, Telefone, WiFi, GPS, GPRS, EDGE, 3G, InfraRED, FM Transmitter, FM Receiver, A/V.	Não (mas tem uma API para isso, portanto depende do vendor do software. Péssimo pois fica despadronizado).
Controle de Interações do Usuário	Sim, 9 itens (interprocessos, dispositivos, acesso a mídia, módulos, temas, teclas, filtros, gravações e timer de segurança).	Não.	Não.	Não (mas tem uma API para isso, portanto depende do vendor do software. Péssimo pois fica despadronizado).

Controle de Dados do Usuário.	Sim, 4 itens (e-mail, pin, arquivos, chaves).	Não.	Parcial, e-mail e documentos (aplicação no repositório extras-testing). Além de caixas postais no servidor IMAP seletivamente.	Não.
Controle Granular de Comportamento por Aplicativos.	Sim, 6 itens de conexão, 9 de interações, 4 de dados do usuário.	Não	Não.	Não. Em tese existe uma API para isso.
Compactação de conteúdo.	Sim.	Não	Não	Não.
Proteção seletiva de conteúdo (criptografia)	Sim, 2 níveis, inclui lista de contatos no segundo nível.	Não.	Disponível em repositório padrão, seletivo por sistema de arquivos/diretórios.	Não.
Senha mestra de criptografia para outras senhas.	Sim.	Não.	Disponível no extras-testing.	Experimental, por linha de comando.
Firewall	Sim, por aplicação Itens disponíveis: SMS, PIN, BIS, BES, E-mail.	Não.	Não (sim, com *kernel* alternativo não oficial. Muito arriscado).	Não.
Limpeza de memória volátil (evitar ataques de *cold boot*).	Sim, configurável: manual, por tempo de inatividade, quando colocar no estojo.	Não.	Não.	Não.
Controle S/MIME	Sim.	Não.	Não.	Não.
TLS Customizável	Sim, autorizações parcialmente seletivas.	TLS suportado mas não customizável.	TLS suportado mas não customizável.	TLS suportado mas não customizável.
Display de informações do proprietário e conformidade com PSI Corporativa.	Sim, 256 caracteres.	Sim, 16 caracteres.	Sim, 32 caracteres.	Sim, 16 caracteres.
Senha de acesso.	Sim. Timeout configurável	Sim. Timeout configurável	Sim. Timeout configurável.	Sim. Timeout configurável.
Controle de Conectividade automática.	Sim.	Parcial.	Sim.	Sim
Messenger Policy	Apenas BB Messenger.	Não.	Sim para MSN (pecan extras-testing) e Gtalk (nativo, linha de comando).	Não.
BlueTooth Policy	Sim.	Não.	Não.	Não.
Browser Policy	Sim.	Não.	Não	Não.

C/MIME, S/MIME Policy	Sim.	Não.	Não.	Não.
Location Based Policy	Sim.	Não.	Não.	Não.
MDS Policy	Sim.	Não.	Não.	Não.
Password Policy.	Sim.	Não.	Sim.	Não.
PGP Policy	Sim.	Não.	Parcial (extras-testing).	Não.
App Policy	Sim.	Não.	Parcial (rotinas Command Line).	Não.
WTLS Policy	Sim.	Não.	Sim.	Não.
GPS "track me home"	Sim.	Não.	Sim.	Não.
Bloqueio Remoto	Sim.	Não.	Sim, por SMS e e-mail.	Não.
Reflash Remoto.	Não.	Não.	Sim, por SMS e e-mail.	Não.
Extensões de Segurança padrão militar (POSIX.1e – MAC, RBAC)	Não.	Não.	Parcial, SELinux com extensão de kernel.	SELinux experimental.
Assinatura / Validação de assinatura de arquivos e aplicações	Sim.	Parcial para arquivos, sim aplicações	Sim.	Sim, mas não considera PKI. Péssimo. Gera confusão e falsa sensação de segurança.
WiFi Security Moderna (WPA2, mínimo)	Sim.	Sim.	Sim.	Sim.
VPN	Sim.	Sim.	Sim.	Sim.
Controle de Acesso DAC Extendido	Não.	Não.	Sim. Mas apenas linha de comando.	Não.
PONTUACÃO	**70**	**16**	**42**	**18**

3 - Conclusões.

O BlackBerry da fabricante RIM é o que tem o maior número de recursos de segurança disponíveis, e a maioria desses recursos foram projetados pensando especificamente no uso corporativo dos dispositivos. A gama de controle e configurações do BlackBerry é granular e amplamente disponível.

O iPhone da Apple evoluiu consideravelmente e hoje apesar de dispor de uma quantidade relativamente interessante de recursos de segurança configuráveis,é dentro os dispositivos avaliados o menos adequado; não está preparado para uso corporativo ainda, e não consegue oferecer conformidade com a maior parte das políticas de segurança corporativa baseadas em frameworks como BS7799 / NBR ISO-IEC 27001 ou requisitos de segurança CobIT.

Os dispositivos baseados em Linux avaliados oferecem alguns destaques relevantes como a inclusão, ainda que de forma experimental, de extensões de controle de acesso ao modelo DAC tradicional e componentes POSIX.1e fracamente aderentes, baseados em SELinux.

O dispositivo da Nokia, baseado em Maemo, destaca-se por permitir bloqueio remoto bem como *reflash*, incluindo remoção de dados. Destaca-se também por tirar proveito do modelo aberto adotado, o que reflete na quantidade de recursos disponíveis por terceiros nos diversos repositórios adicionais e experimentais disponíveis. Apesar de não oferecer a maioria dos recursos de segurança por padrão, sua customização / adição através de aplicações disponíveis em repositórios integrados torna este a segunda melhor opção em número de recursos de segurança disponíveis.

O Android do Google destaca-se por uma API que permite customização dos recursos que cada aplicação pode acessar. Pode ser configurado em arquivos XML (*manifest*). No entanto é precário quando comparado com o controle oferecido pelo BlackBerry. Apesar de ser o mais novo dos sistemas avaliados, seu desenvolvimento é rápido e hoje já é uma opção mais adequada para uso corporativo que o popular iPhone. Há no entanto um desconforto. O Android verifica a assinatura digital de toda aplicação, mas não honra a PKI. Ou seja não valida a assinatura por uma autoridade certificadora conhecida e nem faz distinção quando a CA não é conhecida, tratando todos aplicativos assinados da mesma forma, o que gera uma falsa impressão de segurança e pode ser utilizado para engenharia social, facilitando o convencimento de que a aplicação é segura por ter sido assinada, ainda que assinada por uma CA não conhecida/confiável.

3.1 - Quanto ao uso dos recursos em ambiente corporativo.

O uso adequado de todos os recursos do Black Berry em ambiente corporativo depende da aquisição do BES (Enterprise Server). O uso adequado de todos os recursos do iPhone em ambiente corporativo depende do Mac OS X Server Leopard. O uso adequado de todos os recursos do Maemo em ambiente corporativo depende de customizações de rotinas em ambiente Open Source (*shell scripting*, *python scripting*). O uso adequado do Android em ambiente corporativo é inviável no momento, devido a necessidade de explorar a API de segurança do Android na forma de desenvolvimento.

O Autor

Patrick Tracanelli, especialista (pós-graduação) em Unix/Linux pela Universidade da Califórnia, Berkeley (EDP 302679), especialista (pós-graduação *lato*) em Gestão de Segurança da Informação pela Universidade FUMEC. É profissional Certificado BSDA, certificado CISSP, certificado Citrix Metaframe. Tem interesse especial em pesquisa de sistemas aderentes à POSIX.1e e Common Criteria/EaL. É fundador e sócio-diretor da FreeBSD Brasil LTDA.