
Considerações de segurança no uso de PDA como terminais móveis para aplicações confidenciais e de acesso reservado

C. Julião Duartenn
Oblog Software, SA
juliao.duartenn@esdata.pt

O uso de terminais móveis abre novos campos para a automatização e informatização de um vasto conjunto de actividades. No entanto, esta abertura não está isenta de riscos. Os terminais móveis, concretamente os computadores de bolso (PDA) não possuem nem as capacidades de um computador tradicional nem os mecanismos de segurança adequados à sua natureza móvel, transportável, fácil de perder e sujeita a roubos.

Por outro lado, as redes que suportam a comunicação com estes terminais estão ainda longe de apresentar per si um grau de segurança compatível com a utilização de PDA para aplicações confidenciais ou críticas.

Em terceiro lugar, os sistemas de informação das empresas foram desde sempre desenhados para operar dentro de redes isoladas, seguras e controladas, não estando preparados para sofrer uma abertura a um universo de utilizadores remotos sem que a sua segurança seja reforçada.

Neste documento abordamos os desafios que se colocam do ponto de vista de segurança, apontando formas seguras de implementar estas tecnologias face ao estado da arte dos sistemas actuais, permitindo colher os benefícios da mobilidade sem aumentar o risco operacional associado à tecnologia.

1 Introdução

O uso de terminais móveis abre novos campos para a automatização e informatização de um vasto conjunto de actividades.

O sistema de informação deixa, por um lado, de estar confinado aos limites físicos dos edifícios, podendo seguir o utilizador na sua actividade, onde quer que ela decorra. Por outro lado, mesmo a utilização in-doors se transforma, deixando o utilizador de orbitar em torno do computador, e este torna-se num recurso permanentemente à disposição.

Os sistemas informáticos tem progressivamente vindo a substituir os suportes em papel ao longo dos últimos anos. O papel, em tempos o único meio de suporte de informação, foi lentamente dispensado, à medida que novas aplicações e novos formatos computacionais surgiam.

Mas esta substituição não cobre ainda todas as situações: os computadores são ainda dispositivos fixos, e qualquer utilizador com requisitos de mobilidade é ainda forçado a tomar notas em papel e a introduzi-las posteriormente no sistema informático. Os efeitos disto são a dois níveis:

- Alguma informação, embora registada em papel, não é transcrita para o sistema de informação
- Existem atrasos no registo da informação, no tempo que decorre entre a sua recolha e o seu registo no Sistema

Além disto, o utilizador com necessidades de informação no terreno é forçado a levar consigo conjuntos de informação por vezes de elevada dimensão, de forma a dispor, na sua actividade, de informação de consulta.

O transporte de informação para o terreno já ocorre hoje mediante suportes informáticos,

nomeadamente através de computadores portáteis. No entanto, existem quatro problemas principais com esta abordagem:

- Desactualização da informação, desde que é carregada no portátil até ao momento da consulta
- Necessidade de sincronização frequente da informação entre o sistema central e o portátil
- Necessidade de criar formatos específicos de armazenamento da informação no portátil, uma vez que este nem sempre suporta o formato nativo da informação no sistema central
- Necessidade de presciência quanto à informação necessária: uma vez que as capacidades de armazenamento do portátil são limitadas, a informação que efectivamente vai para o terreno necessita de ser pré-seleccionada e carregada no portátil – a informação que existe no terreno é parcelar e incompleta

Associadas a estas questões surgem outras, de natureza prática e logística, que contribuem para a necessidade de proporcionar novos mecanismos e dispositivos de trabalho aos colaboradores da empresa com necessidades de mobilidade.

O elevado peso e dimensões dos computadores portáteis conjugam-se assim com a recente evolução dos computadores de bolso (PDA), que são já hoje uma solução viável de acesso.

A reduzida capacidade de armazenamento dos PDA faz com que estes nunca tenham sido uma alternativa completa para funcionamento offline. No entanto a recente evolução das redes wireless, dos paradigmas Web e dos mecanismos de compressão e encriptação altera este cenário, e faz do PDA uma plataforma desejável para utilização enquanto dispositivo de acesso remoto a aplicações centralizadas.

2 A Segurança nos PDA

Os PDA apresentam do ponto de vista de segurança um conjunto de desafios único. Os desafios advêm principalmente de:

- A natureza portátil dos PDA
- A reduzida capacidade de processamento quando comparada com um PC normal
- A limitada capacidade de adicionar hardware específico

- Pouca segurança do Sistema Operativo dos PDA
- O uso de redes wireless

2.1 Questões relacionadas com a mobilidade física

A segurança física de um sistema é um factor de extremo relevo na segurança total, na medida em que pode condicionar severamente o tipo de mecanismos de segurança a impor no acesso à informação e às aplicações.

A segurança física de um sistema é relevante a dois níveis:

2.1.1 Integridade do Sistema

Trata-se de um equipamento móvel, ao qual é possível o acesso por partes não autorizadas. Estas partes podem alterar e manipular o PDA, tanto do ponto de vista físico como do ponto de vista de software e configurações.

Os PDA existentes no mercado não apresentam qualquer garantia de resistência a manipulação física. Como tal, a segurança do sistema de informação não deve confiar na integridade física do PDA.

2.1.2 Disponibilidade do Sistema

Sendo um equipamento portátil, apresenta maior probabilidade de ser perdido, roubado ou danificado que um equipamento de secretária ou mesmo que um PC portátil. Devem ser acautelada a necessidade de emitir a um dado utilizador um novo equipamento e respectivas chaves de acesso, em virtude de o anterior se ter perdido ou danificado. Deve igualmente ser possível barrar selectivamente o acesso a um equipamento que tenha sido dado como perdido ou roubado.

2.1.3 Confidencialidade do Sistema

Sendo um equipamento portátil, apresenta maior probabilidade de ser perdido ou roubado. A perda ou roubo do PDA pode levar a que este caia nas mãos de terceiros. É vital impedir que estes possam ter acesso a qualquer informação confidencial, ou que facilite o acesso a informação confidencial. Idealmente, o PDA não deve armazenar qualquer tipo de dados confidenciais ou de negócio. Todos os dados armazenados devem ser encriptados de forma imune a ataques por força bruta.

2.1.4 Acessibilidade do Sistema e Controle de Acessos

Num sistema portátil, é impossível limitar quem tem acesso físico ao equipamento. Assim, é impossível determinar se o utilizador que se apresenta perante o sistema é ou não bem intencionado.

A necessidade de identificar inequivocamente o utilizador é assim muito maior sobre um PDA do que o seria sobre um equipamento localizado fisicamente nas instalações da empresa. Num PDA, um utilizador mal intencionado tem à sua disposição todos os meios físicos e todo o tempo desejado para obter ilicitamente acesso ao sistema.

2.2 Questões relacionadas com a capacidade de processamento

Num PDA, a capacidade de processamento e de memória RAM é inferior à de um PC, o que pode condicionar seriamente o tipo de funções computacionais que o PDA pode efectuar.

No caso concreto da criptografia, a reduzida capacidade computacional do PDA pode condicionar o tipo de algoritmos e a dimensão das chaves usadas. Tal questão deverá merecer especial atenção.

2.3 Questões relacionadas com limitações do hardware

A plataforma PDA dispõe de reduzida conectividade para periféricos dedicados, nomeadamente no capítulo dos equipamentos de segurança. Não é assim viável de momento a concepção de sistemas baseados em PDA que façam uso de reconhecimento de impressões digitais, voz ou retina. O próprio reconhecimento de assinaturas caligrafadas é dificultado pela fraca sensibilidade dos sensores de pressão dos PDA. O uso de sistemas de autenticação por reconhecimento de imagens é prejudicado pela baixa resolução do écran.

2.4 Questões relacionadas com limitações do sistema operativo

O mercado de PDA é actualmente dominado por duas plataformas, Palm e Pocket PC. Nenhuma delas oferece, ao nível do sistema operativo, mecanismos de segurança apropriados à manipulação de informação confidencial e de negócio.

Para tal contribui o facto de não existir ao nível do sistema operativo o conceito de utilizadores e permissões diferenciadas, tornando o PDA numa plataforma onde qualquer utilizador ou aplicação tem livre acesso a qualquer informação armazenada.

Para permitir o uso enquanto plataforma de acesso a aplicações empresariais, estas limitações deverão ser ultrapassadas mediante a adição de software específico e a encriptação de toda a informação e configurações sensíveis.

2.5 Questões relacionadas com o uso de redes wireless

A natureza móvel do PDA faz com que a exploração do seu potencial ocorra primariamente quanto ligado a redes móveis de dados.

O PDA irá comunicar, em primeira instância, com um dispositivo de comunicações, geralmente um telemóvel, e, através deste, com os servidores aplicativos.

Esta última comunicação, de longa distância, entre o utilizador e os servidores aplicativos ocorrerá, de acordo com os standards do mercado, sobre GPRS ou, futuramente, sobre UMTS.

A função de telemóvel (disponibilizando a comunicação GPRS) poderá ser disponibilizada por um equipamento separado ou, eventualmente, estar incorporada no próprio PDA.

Caso esta funcionalidade se encontre num equipamento separado do PDA, a comunicação entre ambos será assegurada, idealmente, via um protocolo wireless de curto alcance, concretamente sobre Bluetooth. O uso de cabos nesta situação iria dificultar a utilização do PDA.

A conexão do PDA directamente a redes wireless (802.11b, Wi-Fi) embora tecnicamente possível, não é aconselhada uma vez que a reduzida capacidade das baterias e o elevado consumo dos dispositivos 802.11b limita seriamente a autonomia do PDA.

Tanto na tecnologia Bluetooth como na tecnologia GPRS existem mecanismos de encriptação de dados. No entanto, ambos apresentam limitações.

A encriptação GPRS apenas protege o troço de comunicação dentro da esfera do operador

móvel. Tanto a comunicação do PDA com o telemóvel como a comunicação a jusante, entre o operador móvel e os servidores aplicativos, não é protegida por esta encriptação. O próprio nível de confidencialidade e encriptação dos dados é dependente da implementação efectuada pelo operador.[CHA02]

A encriptação Bluetooth, além de não apresentar níveis de robustez elevados [JAK01], aplica-se igualmente apenas ao troço entre o PDA e o telemóvel, pelo que a sua utilização deve apenas ser vista como complementar a formas de segurança mais amplas e abrangentes.

3 Recomendações de segurança para a utilização de PDA no acesso a aplicações confidenciais ou de negócio

De forma a assegurar níveis adequados de confidencialidade e integridade no uso de PDA para acesso a informação confidencial ou de negócio, devem ser tomadas medidas de segurança que permitam responder aos desafios específicos dos ambientes móveis e wireless, colmatar as falhas de implementação dos mecanismos de segurança dos PDA e redes móveis, e assegurar um elevado nível de segurança sem restringir ainda assim a funcionalidade da plataforma e a flexibilidade da sua utilização.

3.1 Autenticação de Utilizadores

Os utilizadores deverão ser univocamente identificados e autenticados no sistema, usando mecanismos de autenticação forte, combinando eventualmente dois factores de autenticação.

3.1.1 Não Integração com Login Único

O sistema de autenticação de utilizadores não deverá ser integrado em mecanismos uniformes de login único, uma vez que os requisitos habituais destes sistemas são demasiado fracos para suportar a identificação de utilizadores remotos, sendo geralmente baseados apenas em userid/password.

O facto de a maioria dos mecanismos de login único estarem concebidos para ambientes de rede local com utilizadores conhecidos e necessidade de acesso físico para ensaiar ataques baseados em passwords faz com que não seja recomendável a integração. A excepção possível ocorre caso os mecanismos de login único existentes suportem

autenticação forte baseada em dois factores de autenticação.

3.1.2 Autenticação por Dois Factores

Uma vez que se trata de um sistema distribuído no qual é fácil o acesso de terceiros a equipamentos do sistema (os PDA), a autenticação dos utilizadores do sistema deve ser baseada em dois factores.

O primeiro factor poderá ser uma combinação userid/password. O software dos PDA não deverá possibilitar sob qualquer forma o armazenamento quer do userid quer da password entre sessões.

O segundo factor poderá ter diversas formas, sendo aconselhável baseá-lo no vector “posse”. Existe, no caso dos PDA, um risco inerente aos factores baseados na posse: é provável que os utilizadores armazenem sistematicamente o factor de autenticação junto do PDA, fazendo com que em caso de perda ou roubo o factor de autenticação seja irrelevante. Assim, caso se opte por um factor baseado em posse, os utilizadores sejam adequadamente formados no sentido de manter o PDA e o factor de autenticação sempre separados.

Exemplos de factores de autenticação apropriados para este caso são os RSA SecureID em formato adequado para porta-chaves (facilitando a separação física).

3.1.2.1 Uso do PDA como Factor de Autenticação

O próprio PDA pode ser usado como factor de autenticação. Esta abordagem representa menor segurança que um token físico do género SecureID, mas apresenta menor custo e necessidade de formação.

Para tal é necessário que cada PDA seja equipado com um certificado digital de encriptação, e seja centralmente armazenada a combinação válida de user/PDA autorizada.

Por outras palavras, a cada utilizador será distribuído um PDA com um certificado específico, e esse user só poderá aceder à aplicação a partir desse PDA específico. Além disso, nesse PDA só esse user estará autorizado a aceder ao sistema.

Tal permite facilmente limitar o tempo de exposição a ataques externos por roubo ou perda de um PDA, uma vez que o certificado do PDA roubado pode ser imediatamente

revogado assim que o utilizador reporte o acontecimento.

O uso do PDA como factor de autenticação é vivamente recomendado, complementado ou não com um segundo factor físico de autenticação. O factor userid/password deverá em todos os casos estar presente.

3.1.3 Regras de Gestão de Passwords

As passwords deverão ter um mínimo de 8 caracteres e incluir obrigatoriamente letras e números. A password deverá ser alterada com periodicidade não inferior a 45 dias. Na alteração de passwords, a nova password deverá ser submetida a validação estatística ou de dicionário (usando, por exemplo, o crack), de forma a determinar a sua robustez.

3.2 Identificação de Devices

Os PDA devem estar univocamente identificados de forma a garantir tratar-se de equipamentos registados e evitar a intrusão de equipamentos de terceiros no canal seguro.

3.2.1 Identificação Unívoca de PDAs

Em cada PDA deve ser instalado um certificado digital usado na encriptação das comunicações com o servidor aplicacional.

Este certificado deve ser único para cada PDA, e funcionar com identificador do dispositivo de acesso usado. Em caso de roubo ou perda de um PDA o certificado pode ser revogado, impedindo assim terceiros de abusar do equipamento.

Poderá ainda revelar-se útil para efeitos de auditoria.

3.2.2 Identificação Unívoca de Telemóveis

Cada telemóvel numa rede digital encontra-se já identificado por via do seu IMSI, o que permite teoricamente a limitação do acesso a determinados endereços ou serviços a um grupo de equipamentos.

Esta abordagem, que pode encontrar um paralelo na criação de uma VLAN sobre GSM/GPRS, necessita no entanto de colaboração activa do operador móvel, pelo que carece de negociação com este.

Poderá ser investigada, na medida em que impede que telemóveis e outros equipamentos GPRS tentem interferir no canal de comunicação da aplicação.

3.2.3 Identificação de Pares de Devices

No caso em que seja viável proceder à identificação unívoca de telemóveis, é igualmente possível cruzar o endereço atribuído ao telemóvel pelo operador com o certificado apresentado pelo PDA na comunicação com o servidor.

Tal permitirá averiguar uma correspondência de um para um entre PDA e telemóvel, contribuindo assim para uma segurança acrescida na medida em que terceiros só terão capacidade de tentar o acesso ao sistema caso detenham simultaneamente o PDA e o telemóvel associado (aplicando-se naturalmente ainda a necessidade de conhecer um userid/password ou outros factores de autenticação).

3.3 Confidencialidade dos Dados em Trânsito

De forma a assegurar a confidencialidade e integridade dos dados em trânsito, estes deverão ser sempre encriptados em todo o trajecto entre o PDA e o servidor aplicacional, uma vez que nem a encriptação do Bluetooth nem a encriptação do GPRS garantem confidencialidade em todo o trajecto da informação, incluindo na rede do operador telefónico e entre esta e o servidor aplicacional.

3.3.1 Encriptação End-to-End

O sistema deverá usar SSL 3, de 128 bits ou superior, com certificados no servidor e em todos os clientes. Cada cliente (PDA) deverá dispôr de um certificado individual e único, que validará a máquina e não o utilizador. Os certificados poderão ser emitidos pela entidade gestora do sistema. O servidor respeitará obrigatoriamente uma Certificate Revocation List.

A instalação dos certificados poderá ser feita manualmente na preparação de cada PDA.

3.3.2 Encriptação Forte

O sistema deverá usar SSL de no mínimo 128 bits de encriptação, usados para gerar uma chave de sessão de no mínimo 1024 bits.

A implementação de SSL pode ser disponibilizada quer por um browser adequado quer por módulos criptográficos (RSA, etc) integrados numa aplicação a desenvolver.

O uso de encriptação forte no PDA pode levantar problemas de capacidade de CPU, pelo que deve ser cuidadosamente seleccionada uma implementação eficaz do ponto de vista criptográfico e eficiente do ponto de vista de recursos.

3.4 Segurança e Arquitectura de Rede

3.4.1 Troço PDA-Telemóvel

O PDA deverá usar Bluetooth para comunicar com o telemóvel. Ambos os equipamentos devem reconhecer-se como Trusted Devices ao nível do protocolo Bluetooth. Nenhum dos equipamentos deverá permitir qualquer tipo de comunicação com “untrusted devices”. A comunicação ao nível do protocolo deve ser encriptada. A troca inicial de chaves entre os devices deve ser efectuada num ambiente seguro.

3.4.2 Troço Telemóvel-Operador

O telemóvel usará GPRS para comunicar com o Operador. O operador deverá disponibilizar GPRS em modo encriptado.

Será interessante se o operador disponibilizar a criação de um “closed user group” para tráfego GPRS, incluindo os telemóveis deste sistema e um gateway específico, com IP dedicado.

3.4.3 Troço Operador-Servidor Aplicação

O operador comunicará com o Servidor da aplicação sobre uma rede IP, encaminhando para ele todo o tráfego dos PDA.

3.4.3.1 Troço Op.-Serv. Apl. - Dedicado

Poderá existir uma linha dedicada (FR, HDLC) entre o operador e o site de produção. Nesse caso, todo o tráfego circula em linhas autónomas, excepto na rede do operador.

3.4.3.2 Troço Op.-Serv. Apl. - Internet VPN

O operador poderá encaminhar o tráfego para o servidor aplicacional sobre uma VPN IPSEC

estabelecida entre o gateway do operador e a firewall do site de produção.

3.4.3.3 Troço Op.-Serv. Apl. - Internet Clear

O operador poderá encaminhar o tráfego para o servidor aplicacional sobre a internet, sem encriptação adicional. Existe neste caso a necessidade de minimizar o tipo de ataques de spoofing que possam ocorrer contra o servidor aplicacional.

3.4.4 Arquitectura do Site de Produção

O site de produção no qual está instalado o servidor aplicacional deverá estar protegido com dois níveis de firewall, sendo o primeiro implementado por filtragem simples no router de entrada e o segundo disponibilizado por uma firewall de nível 5.

O servidor aplicacional deve disponibilizar o acesso à aplicação PDA apenas num ip/port específico, e deve filtrar todo o tráfego para esse port, permitindo apenas acessos oriundos do gateway do operador.

A aplicação deve ser disponibilizada exclusivamente sobre SSL 3, com validação obrigatória de um certificado de cliente válido.

3.5 Controle do Acesso à Aplicação no Servidor

O servidor deve condicionar sempre o acesso à aplicação mediante a validação do certificado e a apresentação de userid/password válido.

O acesso de um dado utilizador deve ser bloqueado por 15 minutos em caso de 3 tentativas erradas de login. O acesso de um dado utilizador deve ser bloqueado permanentemente em caso de três bloqueios temporários num período de 24 horas. O acesso pode ser desbloqueado mediante pedido do utilizador, validado de forma forte. Não deve ser autorizado um pedido de desbloqueamento não validado de forma forte.

A validação forte do pedido de desbloqueamento de password deverá ser feita mediante procedimentos a determinar. No entanto, nunca deverá ser suficiente uma chamada telefónica para um helpdesk nem o mero envio de um fax.

3.6 Controle do Acesso à Aplicação no PDA

O PDA é um ponto crítico da segurança do sistema. Não obstante a validação de userid/password no servidor, deverá ser tida especial atenção à utilização da aplicação cliente no PDA, mesmo que esta seja apenas um browser. A própria “history” do browser pode fornecer informação indesejada.

O PDA deve ser equipado com um sistema de autorização de acesso forte. Este sistema, implementado em software, deve:

- Solicitar password sempre que o PDA é ligado, não permitindo a sua utilização sem uma password válida
- Permitir controlar as aplicações que são lançadas, solicitando uma password para lançamento do browser ou da aplicação cliente
- Encriptar selectivamente toda a informação armazenada no PDA (nomeadamente dados de negócio inscritos em documentos, folhas de calculo, etc)

3.7 Limitação de Trojans e Outros no PDA

A segurança do PDA pode ser comprometida por aplicações nele instaladas, quer se trate de vírus ou outro tipo de aplicações maliciosas. É trivial a instalação num PDA de aplicações de captura de texto introduzido, que permitirá a terceiros conhecer o userid e password de um dado utilizador. Instalada uma aplicação deste género, o terceiro terá apenas que ter acesso ao PDA para consultar o userid/password capturado e introduzir-se no sistema.

Assim, é vital limitar a capacidade de instalar aplicações não autorizadas no PDA. O PDA deverá ser equipado com software que permita impedir a instalação e/ou execução de aplicações não autorizadas.

3.8 Encriptação da Informação Local

Além do acesso à aplicação central, o PDA pode ser usado para armazenar e tratar localmente outro tipo de informação confidencial ou de negócio.

Esta informação poderá ser ou não suficiente para comprometer a confidencialidade e integridade do sistema.

Como tal, o PDA deve ser equipado com software que permita a encriptação dos dados do utilizador, quer se trate de notas em

formato de texto, de folhas de cálculo ou de outro tipo de informação.

Os utilizadores deverão ser formados quanto à necessidade de proteger a informação e aos processos à sua disposição para o fazer.

3.9 Auditoria do Sistema

O sistema deverá ser objecto de auditorias de segurança periódicas.

Tais auditorias visarão detectar vulnerabilidades e falhas no sistema, bem como nos processos que lhe estão associados.

As auditorias poderão envolver não só a componente servidora como a componente aplicacional, os serviços prestados pelo operador móvel e a configuração dos PDA.

3.10 Monitorização do Sistema

O sistema deverá ser objecto de monitorização de segurança, tanto ao nível de rede e sistema como ao nível funcional e aplicacional. Ao nível de rede e sistema esta monitorização materializar-se-á na detecção continuada de vulnerabilidades, perfis de tráfego (detecção de intrusões) e níveis de resposta do sistema. Ao nível funcional e aplicacional a monitorização consistirá no controle estatístico dos trends funcionais, acompanhada de relatórios que permitirão aferir e fixar estes trends, detectando desvios e anomalias que permitam despoletar actividades de auditoria.

4 Conclusão

O uso de PDA no acesso a aplicações de negócio e informação confidencial não é isento de riscos. No entanto, é viável enquanto potenciador do negócio desde que sejam tomadas as medidas adequadas de protecção e segurança.

Estas medidas são a 4 níveis:

- Reforço da segurança no próprio PDA
- Autenticação e Encriptação forte
- Rigor na implementação de servidores e aplicações
- Rigor nos procedimentos e na formação dos utilizadores

Complementadas com adequada monitorização e auditoria, as directrizes apontadas neste documento permitem

implementar uma infraestrutura segura e dinâmica de suporte a uma força de trabalho móvel, sem comprometer a confidencialidade da informação nem as funcionalidades da solução.

Consideradas do ponto de vista da análise de risco, as directrizes apresentadas, se seguidas, minoram o risco de segurança informática da solução ao ponto de a tornar viável, tanto do ponto de vista económico como do ponto de vista do risco global da empresa.

Referências

CHA02: Dung Chang, Security Along the Path Through GPRS Towards 3G Data Services, SANS Institute, 2002

JAK01: Jakobsson, Markus; Wetzel, Sussane, Security Weaknesses in Bluetooth, Bell Labs, 2001

