

Segurança em redes móveis

Pedro Moritz de Carvalho Neto
pedro@fazion.com.br

Introdução

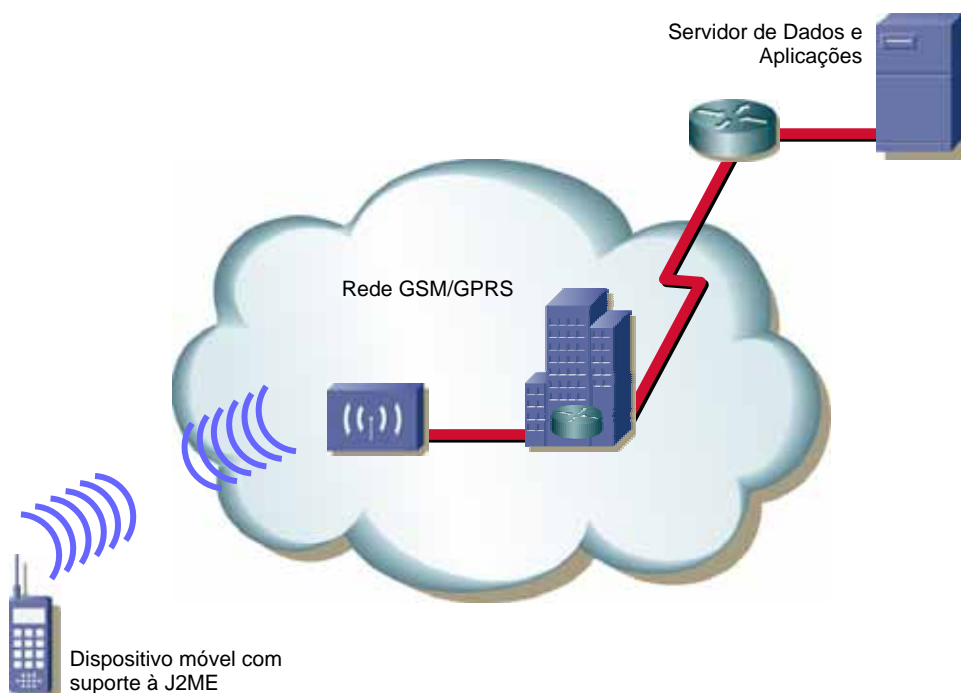
Este artigo trata dos aspectos de segurança relacionados à transferência de dados através de uma rede móvel, como é o caso da telefonia celular. Ainda há muitas preocupações sobre os critérios de segurança que envolvem a transmissão por uma rede móvel e, como veremos no texto, a rede é segura e permite aplicações de alta complexidade, sem riscos para as empresas e suas informações.

Os três elementos da segurança

Nos sistemas da FAZION existem três elementos que devem ser considerados quando se fala de **segurança da informação**:

- o primeiro elemento é a aplicação que reside no dispositivo móvel do usuário;
- o segundo elemento é a aplicação que reside em um servidor, na infra-estrutura de Tecnologia da Informação e Comunicação – TIC – do cliente ou da FAZION, e que troca dados com o dispositivo móvel;
- finalmente há o terceiro elemento, que é a rede GSM (*Global System for Mobile Communications*) / GPRS (*General Packet Radio Service*), utilizada para o transporte de dados.

A figura abaixo representa, de forma esquemática, como tais elementos estão relacionados na rede.



A seguir analisamos esses três elementos, e como impactam na segurança da comunicação.

O **primeiro elemento** é uma aplicação construída com tecnologia Java™, da SUN Microsystems™¹, devidamente instalada no dispositivo móvel do cliente. Esse dispositivo móvel tipicamente é o **telefone celular**. A aplicação armazena localmente, na memória não-volátil do celular, os dados que foram recebidos ou que posteriormente serão enviados a um servidor. Esses dados, enquanto armazenados, estão seguros e invioláveis, devido aos mecanismos de segurança proporcionados pela plataforma Java™, além do uso da criptografia, visando a confidencialidade dos dados armazenados.²

O **segundo elemento**, que é a aplicação residente em um **servidor** e que se comunica com o dispositivo móvel, é seguro por

¹ "Sun™, Java™ e J2ME™ são marcas registradas da Sun Microsystems, Inc. nos E.U.A. e em outros países."

² A Fazion faz parte do *Partner Advantage Program da Sun™* para ISVs (*Independent Software Vendors*).

um mecanismo de autenticação. Isto significa que, a cada tentativa de troca de dados com o servidor, o dispositivo móvel precisa enviar um *login* e uma senha para autenticação. Se esses dados forem confirmados pelo servidor, a troca de dados se dará sem problemas. Caso sejam enviados dados de autenticação incorretos, a tentativa ficará registrada e não serão trocadas informações entre o dispositivo móvel e o servidor. É possível também implementar outros níveis de segurança que associem o *hardware* do aparelho celular utilizado através do seu IMEI (*International Mobile Equipment Identity*, código que identifica de maneira única os telefones celulares GSM) ou através do uso de certificados digitais.

O **terceiro elemento** é a rede GSM/GPRS, de responsabilidade da operadora do serviço de telefonia móvel contratado. A tecnologia na rede GSM/GPRS possui muitos recursos de segurança, entre eles a autenticação da rede com o equipamento do usuário. Um dos pontos importantes do GSM/GPRS é a **criptografia** dos dados transmitidos. Neste caso, a criptografia é feita através de uma chave simétrica. Significa que tanto o dispositivo móvel quanto a rede GSM/GPRS compartilham uma informação (que é a chave simétrica), utilizada para criptografar a informação antes de ser enviada.

Outro fator importante é que os sistemas da FAZION utilizam o protocolo TCP/IP, que é um protocolo de rede confiável e robusto, sobre a rede GPRS. Isto garante a integridade do dado que circula na rede, e garante que o dado que será lido pelo servidor foi o mesmo dado enviado pelo celular.

Existe um ponto de vulnerabilidade neste caminho, que é o momento em que o dado sai do sistema GSM/GPRS e entra na rede local da operadora, com o objetivo de acessar a Internet. Deste ponto, até o momento em que o dado chega até o servidor de dados, ele "poderia" ser lido. No entanto este fato não significa que o dado possa ser facilmente acessado. Na verdade, além do conhecimento técnico e da necessidade de acesso físico à rede local da operadora ou do servidor de dados, o conteúdo acessado provavelmente não fará sentido. Por exemplo, uma ordem de serviço cujo encerramento foi enviado ao servidor de

dados pode ser representada da seguinte forma: #34435353#1011#. Ou seja, fora do contexto, fica impossível conhecer o significado do dado capturado. Além disso, é possível estabelecer criptografia entre o dispositivo móvel e o servidor de dados, de ponta a ponta, além da criptografia da rede móvel, por meio do uso de HTTPS (protocolo HTTP com uso de SSL - *Secure Sockets Layer*). Este protocolo proporciona um ótimo nível de confidencialidade, já disponível em diversas implementações do J2ME™ MIDP 1.0, e recurso nativo nos aparelhos celulares que suportam J2ME™ com padrão MIDP 2.0.

Conclusões

Uma análise dos recursos e da segurança das redes de telefonia celular GSM/GPRS confirma a sua escolha como opção correta no transporte de dados corporativos. Além de viável economicamente, é uma escolha bastante interessante, pois é uma rede robusta, com níveis de segurança aceitáveis que podem ser complementados através de recursos como criptografia e autenticação, disponibilizados pela tecnologia Java™.

A FAZION utiliza esses recursos para desenvolver aplicativos de última geração, focados em soluções especiais para o ambiente empresarial.³



³ Veja em www.fazion.com.br alguns aplicativos de demonstração, faça o download, teste e comprove os recursos e facilidades disponíveis.