FIBEDROID: MOBILIDADE COM SEGURANÇA E PRIVACIDADE

Alain Erson Frantz*
Arthur Ewerton Ril Uliana**
Roberson Junior Fernandes Alves***

Resumo

A segurança da informação está diretamente ligada ao sucesso de uma empresa e à privacidade do usuário final. Este artigo visou demonstrar a necessidade de uma aplicação de segurança para o *smartphone* com a finalidade de assegurar a confidencialidade, a integridade e a disponibilidade da informação. O sistema Android possibilita o uso de recursos e informações disponíveis no próprio aparelho para desenvolver aplicações que visam facilitar e aprimorar a segurança ao seu usuário. Tendo como finalidade propiciar maior segurança da informação para empresas e possíveis usuários, o FibeDroid, por meio de métodos remotos ou locais, visualiza sua localização e realiza disparo de alarme e bloqueio, bem como faz *backup* de contatos.
Palavras-chave: Android. Segurança da informação. Mobilidade. FibeDroid.

1 **INTRODUÇÃO**

A computação móvel trouxe mudanças na forma como as pessoas se comunicam e trabalham. Antes, os celulares faziam chamadas de voz, agora, os *smartphones* se tornaram, definitivamente, computadores de bolso. A execução de programas empresariais deixou de ser exclusividade dos *desktops* e *notebooks* passando a ser realidade também em pequenos dispositivos móveis, como os *smartphones* e *tablets*.

Com a portabilidade e o advento da internet de banda larga móvel, 3G e superiores, os usuários podem ficar *on-line* praticamente onde e quando desejarem, criando-se uma ameaça de seus dados e uma necessidade de localização do celular em casos de furto ou perda.

Da mesma forma que os usuários têm a necessidade de proteger suas senhas e documentos, as empresas que disponibilizam *smartphones* para os seus funcionários executarem as tarefas de trabalho também necessitam de segurança para todos os seus *smartphones* distribuídos. Assim, este aplicativo visa explorar e adicionar segurança a celulares e *smartphones* equipados com sistema operacional (SO) Android, fazendo uso dos recursos disponíveis nos próprios aparelhos, como *Global Position System* (GPS) para localizá-lo quando perdido ou roubado e os meios de conexão para transferir informações entre o aparelho e a aplicação servidora.

2 **MOBILIDADE**

Os avanços na capacidade de processamento dos dispositivos móveis aliados ao aumento da autonomia das baterias e maior cobertura de sinal das operadoras vêm tornando estes dispositivos cada vez mais práticos, populares e diversificados, cada qual com seu sistema operacional, como Blackberry OS, Symbian, Windows Phone, iOS e Android.

Assim, além de melhores configurações de *hardware*, surge a necessidade de melhores e mais diversificadas configurações de *software* para atender a um público igualmente diversificado e numeroso, como o mercado brasileiro.

* Acadêmico do Curso de Sistemas de Informação da Universidade do Oeste de Santa Catarina de São Miguel do Oeste; alain061191@hotmail.com
** Acadêmico do Curso de Sistemas de Informação da Universidade do Oeste de Santa Catarina de São Miguel do Oeste; arthurril@hotmail.com
*** Especialista em Ciências da Computação pela Universidade Federal de Santa Catarina; Professor do Curso de Bacharelado em Sistemas de Informação da Universidade do Oeste de Santa Catarina de São Miguel do Oeste; Rua Oiapoc, 211, São Miguel do Oeste, SC; roberson.alves@unoesc.edu.br

2.1 ANDROID

O Android, de acordo com Lecheta (2010, p. 20), "[...] consiste em uma nova plataforma de desenvolvimento para aplicações móveis, e diversas aplicações já instaladas e, ainda, um ambiente de desenvolvimento bastante poderoso, ousado e flexível."

Assim, o Android facilita o trabalho dos programadores de *software* para dispositivos móveis, permitindo a eles desenvolverem aplicações para tais dispositivos independentemente da marca, tornando as aplicações portáveis entre modelos e ampliando a experiência do usuário ao usar soluções de *software* voltadas a estes dispositivos.

Esses atributos trazem vantagens para os fabricantes, programadores e usuários, pois os fabricantes podem usar e alterar o sistema que será embarcado nos seus dispositivos sem pagar nada por isso, os programadores podem desenvolver para uma única plataforma e atingir vários dispositivos de inúmeras marcas e os usuários serão servidos por uma diversidade maior de configurações de *hardware* sem sacrificarem seus aplicativos favoritos.

Algumas das linguagens de programação que podem ser utilizadas no desenvolvimento de aplicações Android são Python, Perl, JRuby, Lua, BeanShell, JavaScript, C e Java. O Android possui uma máquina virtual *Dalvik* que compila o código Java para arquivos ".dex" e, além da Google fornecer o SDK (*Software Development Kit*) para o desenvolvimento de aplicações em Java, ela também fornece o *Native Development Kit* (NDK), para o desenvolvimento em C.

Conforme pesquisa da *International Data Corporation* (2012), o Android já corresponde a mais da metade dos SOs que equipam os *smartphones* vendidos no primeiro trimestre de 2012.

2.2 SEGURANÇA DA INFORMAÇÃO

A segurança da informação pode ser definida como a proteção de informações de diversos tipos. Sendo a informação um ativo importante para a continuidade dos negócios de uma organização, ela necessita ser protegida adequadamente (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

Para isso, necessita-se de um conjunto de ações que devem assegurar três propriedades básicas da informação: a confidencialidade, a integridade e a disponibilidade, cada uma em maior ou menor grau, dependendo do setor em que a organização atua.

Os usuários precisam ser orientados a usarem com cautela os recursos da computação móvel, pois de acordo com estudo relatado por Rodrigues (2012) "[...] o cibercrime já vê os dispositivos móveis como alvo, pois estão surgindo *malwares* para todas as plataformas."

Com a finalidade de normatizar os processos que venham a agregar segurança às informações armazenadas e manipuladas por empresas e usuários comuns, a ISO *International Organization for Standardization* (ISO) está desenvolvendo uma família de normas de sistema de gestão de segurança da informação (SGSI). Conforme descrito pela Associação Brasileira de Normas Técnicas (2005, p. 7), "A família inclui normas sobre requisitos de sistema de gestão da segurança da informação, gestão de riscos, métricas e medidas, e diretrizes para implementação. Esta família adotará um esquema de numeração usando a série de números 27000 em sequência."

A família de normas ISO 27000 incorporará a ISO 17799 que será esquematizada sob a nova numeração ISO 27002. O Quadro 1 descreve o cenário atual do esquema de numeração de algumas normas da ISO 27000.

Quadro 1 – Normas sob o novo esquema de numeração ISO 27000

ISO 27000	Tecnologia da Informação: Sistemas de gerenciamento da segurança da informação. Visão geral e vocabulário.
ISO 27001	Especificação de um sistema de gestão de segurança da informação (SGSI) que substituiu a antiga norma BS7799-2.
ISO 27002	Nova numeração da antiga ISO 17799.
ISO 27003	Número oficial de um novo padrão que pretende oferecer orientação para a implementação de um Sistema de Gerenciamento.
ISO 27004	Esta norma abrange informações sobre métricas e medições de sistemas de gerenciamento da segurança, incluindo as sugeridas pela ISO 27002.
ISO 27005	Esta norma fornece orientações para o gerenciamento de riscos da segurança da informação em uma organização.
ISO 27006	Estabelece requisitos para organizações que fornecem auditoria e certificação de sistemas de informação de gestão da segurança.
ISO 27011	Orientações de gerenciamento da segurança da informação para telecomunicações.
ISO 27033	Segurança na Rede.

Fonte: adaptado de *International Organization for Standardization* (2009).

De forma complementar ao aplicativo, será elaborado um guia de uso consciente para dispositivos móveis vislumbrando e adequando as normas descritas no Quadro 1, pois a segurança da informação em dispositivos móveis precisa de cuidados diferenciados, mas muitos dos conceitos válidos para *desktops* podem ser aplicados também a plataformas móveis.

2.2.1 **Segurança em dispositivos móveis**

Conforme Dariva (2011, p. 32-33), os celulares já estavam presentes no ambiente corporativo na década de 1990, mas foi a partir de 2005 que os *smartphones* entraram neste ambiente trazendo funcionalidades melhoradas para o dia a dia, porém, também os riscos de um mercado e tecnologia imaturos aliados a uma infraestrutura imprópria e administradores de Tecnologia da Informação (TI) despreparados para oferecer qualidade em serviços móveis.

Os avanços na estrutura de TI móveis e administradores adequadamente qualificados ou soluções terceirizadas chegaram com a maturidade no mercado corporativo entre 2008 e 2010, com a expressão *Mobile Device Management* (MDM) (DARIVA, 2011, p. 33). O MDM, além de permitirem que os administradores inspecionem os dispositivos móveis tão facilmente quanto os computadores *desktops*, visando "[...] otimizar as funcionalidades e a segurança da comunicação entre os dispositivos e a organização [...]" (ROUSE, 2009 apud DARIVA, 2011, p. 35).

Conforme Eleutério e Machado (2010, p. 45): "Dispositivos portáteis, como telefones celulares e PDAs, geralmente contêm uma memória interna que pode armazenar dados de usuários. Além disso, os dispositivos mais recentes já permitem a expansão de memória por meio de cartões de memória." Isso os torna capazes de armazenar grandes quantias de dados que, por exemplo, podem causar enorme prejuízo às empresas que façam uso desse recurso para carregar informações estratégicas a alguma reunião de negócios e tenham o equipamento perdido, roubado ou mesmo que alguém explore alguma vulnerabilidade, como *bluetooth* ou *Wifi*, para obter tais informações.

Para Dariva (2011, p. 45-49), os projetos de MDM devem oferecer funcionalidades específicas para segurança e privacidade das informações, cada uma com vantagens de uso em determinadas situações. São exemplos de funcionalidades MDM o *wipe* (Limpeza remota), o *backup* e a restauração remota, o bloqueio do dispositivo ou parte dos recursos deste, a obrigatoriedade do uso de senhas, a criptografia e o rastreamento.

Além de roubos e extravios, os dispositivos móveis estão sujeitos a praticamente todas as vulnerabilidades e ameaças encontradas nos ambientes estáticos, porém, eles são mais frágeis se considerarmos que a segurança física depende do portador dele e dos lugares por onde este trafegar. Estes fatores exigem mais empenho dos engenheiros para desenvolver projetos com alto padrão de qualidade geral, abrangendo segurança, usabilidade, confiabilidade, entre outras características desejáveis à qualidade.

3 **FIBEDROID**

Com o propósito de aumentar a segurança dos usuários ou das empresas que contratarem os serviços, para cada *smartphone* é gerada uma chave única por meio de atributos inerentes ao dispositivo, como o *Media Access Control* (MAC) físico, *bluetooth* e o *International Mobile Equipment Identity* (IMEI), além de um código próprio do FibeDroid. Tal chave é armazenada no servidor; dessa forma, somente haverá troca de informações mediante confrontação das chaves. Para garantir a transparência do bloqueio de chamadas e SMS, o usuário poderá gerenciá-los manualmente por meio da *blacklist*.

Se necessário, o usuário poderá disparar um alarme do dispositivo via *Short Message Service* (SMS), que somente irá parar mediante toque do usuário na tela do dispositivo, tendo a possibilidade de executar esta ação mediante inserção de um código para parar o alarme.

3.1 REQUISITOS E MODELAGEM

A UML foi adotada como meio de documentação e levantamento de requisitos para o desenvolvimento do FibeDroid. O sistema necessita de alguns requisitos não funcionais para a obtenção da melhor experiência do usuário. Tratam-se de recursos que devem estar presentes no dispositivo que irá executar o FibeDroid, como conexão com a internet (3G, 4G, Wi-Fi), 30 Mb de memória RAM livre, 10 Mb de espaço interno para instalação e dados, 600MHz de processamento (não foram realizados testes em dispositivos inferiores), Sistema de localização global (GPS), Tela sensível ao toque (*touch-screen*), Sistema Operacional Android 2.3.3 (GINGERBREAD, API10) ou posterior.

Com o intuito de exemplificar suas funcionalidades, simplificar e facilitar o desenvolvimento da aplicação foi definido um diagrama de caso de uso. Entre os requisitos funcionais, descritos no diagrama, permeiam o gerenciamento de uma *blacklist* de números e palavras-chave que podem ser bloqueados em chamadas ou mensagens de texto, a funcionalidade de geolocalização e a realização de *backup* dos contatos (apenas com telefone).

O banco de dados nativo do Android é o SQLite, *software* leve e compacto, muito prático para persistir e recuperar informações geradas pelas aplicações Android de forma estruturada, de acordo com a modelagem relacional. Vislumbrando essa facilidade de acesso e manipulação de informações persistentes, foi concebido um diagrama relacional utilizando a ferramenta *Computer-Aided Software Engineering* (CASE) DBDesigner Fork, pois este permite a manipulação visual das tabelas e conta com recurso de exportação para o formato *Structured Query Language (SQL)* específico, retirando, por exemplo, comentários do código SQL.

3.2 DESENVOLVIMENTO

Para que o desenvolvimento possa ser feito independentemente da localização geográfica da equipe, foi utilizado o RiouxSVN, que permite o controle e o gerenciamento de versão do aplicativo e do servidor.

Para o desenvolvimento da versão servidora foi utilizado o NetBeans IDE 7.0, agregando a ele as bibliotecas Jersey, que é a implementação da biblioteca JAX-RS, Gson, para a conversão rápida de objetos no formato Json aos objetos Java e vice-versa, o *driver* JDBC4 para a conexão com o PostgreSQL 8.4 e o EclipseLink, que é a implementação de referência ao JPA2 (*Java Persistence API*).

Por se tratar de um sistema de segurança, necessita-se garantir a confidencialidade da informação, ou seja, garantir que somente usuários com autorização tenham acesso a configurações e funcionalidades do sistema. Para isso, o sistema conta com uma tela de autenticação para ter acesso às funcionalidades.

O aplicativo contém um sistema de localização do celular mediante latitude e longitude, com *Application Programming Interface (API)* do Google que mostrará ao usuário o local que seu dispositivo está. Isso ajudará a localizar o dispositivo em caso de furto ou roubo, ou até mesmo perda, o usuário poderá solicitar de seu próprio dispositivo sua localização.

Para a inclusão do Google Maps no sistema FibeDroid, foi necessária a realização de alguns procedimentos para a obtenção de uma chave de acesso. Primeiramente, gerar uma *hash* MD5 do seu arquivo *.keystore* utilizando o utilitário *keytool* presente no diretório *bin* do Java, em seguida, utilizar esse *hash* para obter o "Maps API key", por meio do *site* do Google destinado a desenvolvedores (https://developers.google.com/android/maps-api-signup?hl=pt-BR), para isso, é preciso ter uma conta no Google.

Uma funcionalidade importante está na realização do *backup* que o usuário pode fazer de seus contatos telefônicos, sendo enviados ao banco de dados no servidor quando existir conexão com a internet, podendo garantir que seus contatos sejam mantidos em caso de furto ou perda de seu dispositivo.

Para o desenvolvimento de testes está sendo utilizado o Android *Software Development Kit* (SDK), que fornece às bibliotecas da API ferramentas de desenvolvimento necessárias para construir, testar e depurar o aplicativo Android. A linguagem escolhida para o desenvolvimento é Java, tendo como IDE o Eclipse e dois *plugins* principais, um deles sendo uma ferramenta para o versionamento, o Subclipse, o outro, o *Android Development Tools* (ADT) que traz facili-

dades no desenvolvimento para Android. Para fins de testes e simulações, faz-se uso do emulador *Android Virtual Device* (ADV), e validações são efetuadas em dispositivos móveis reais.

Muitas vezes, o usuário esquece onde está seu *smartphone*, ou até mesmo acaba roubado; nesse caso, para encontrar facilmente o dispositivo, o FibeDroid conta com um sistema de disparo de alarme, que recebe uma mensagem de texto identificando o código do alarme; este faz com que a configuração de volume do alarme mude para o seu máximo, e entre em um laço de repetição que somente irá parar quando for pressionado o botão de "Parar"; tal botão pode ser facilmente substituído por algum tipo de senha.

4 **CONCLUSÃO**

Com o crescimento tecnológico, os *smartphones* estão ficando capazes de realizar tanto tarefas empresariais quanto para usuários finais, fazendo com que os usuários fiquem conectados quase o tempo todo, trazendo ameaças à segurança da informação.

Os resultados obtidos até então proveem algumas soluções para agregar segurança às informações contidas nos dispositivos móveis, além de proporcionar maior controle sobre a propriedade do aparelho por meio do disparo do alarme de pânico, que pode ser acionado por meio de SMS ou com a inserção de um SIM-Card desconhecido pelo FibeDroid. Também é possível manter um *backup* dos contatos do aparelho, garantindo, assim, a manutenção da sua rede de relacionamentos, e localizar-se geograficamente por meio da API GoogleMaps, utilizando o recurso de obtenção da latitude e longitude por meio do GPS.

O desenvolvimento de aplicações para Android é facilitado pelo suporte nativo ao Java EE; dessa forma, um desenvolvedor leigo em Android, mas com certa experiência em Java, pode criar aplicações personalizadas, como um tocador de musicas ou despertador, com uma curva de aprendizado pequena, pois o Android SDK em conjunto com o Eclipse e o *plugin* ADT fornecem um conjunto de ferramentas muito úteis, inclusive com interface gráfica ao desenvolvimento das telas.

FibeDroid: Mobility with Security and Privacy

Abstract

The security of information is directly linked to the success of a company and to the final user's privacy. This article aimed to demonstrate the need for a security application for smartphone in order to ensure the confidentiality, integrity and availability of information. The Android system allows the use of resources and information available on the device itself to develop applications that aim to facilitate and enhance security for its user. For purposes of providing greater information security for companies and potential users, FibeDroid, through remote methods or locations, displays its location and performs alarm trigger and lock, and also saves contacts.
Keywords: Android. Information security. Mobility. FibeDroid.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 17799** – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005. 120 p.

DARIVA, R. **Gerenciamento de dispositivos móveis e serviços de telecom**: estratégias de marketing, mobilidade e comunicação. Rio de Janeiro: Elsevier, 2011. 134 p.

ELEUTÉRIO, P. M. S.; MACHADO, M. P. **Desvendando a computação forense**. São Paulo: Novatec, 2010. 200 p.

INTERNATIONAL DATA CORPORATION. **Android – and iOS-Powered Smartphones Expand Their Share of the Market in the First Quarter, According to IDC**. 2012. Disponível em: <http://www.idc.com/getdoc.jsp?containerId=prUS23503312>. Acesso em: 27 maio 2012.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION>. **ISO 27000**: Information technology Security techniques – Information security management systems – Overview and vocabulary. 2009. Disponível em: <http://www.27000.org/index.htm>. Acesso em: 15 jun. 2012.

LECHETA, R. R. **Google android**: aprenda a criar aplicações para dispositivos móveis com o android SDK. 2. ed. rev. e ampl. São Paulo: Novatec, 2010. 608 p.

RODRIGUES, R. **Brasil é líder em acesso não autorizado de aparelhos móveis a redes corporativas**. 2010. Disponível em: <http://idgnow.uol.com.br/seguranca/2010/10/28/brasil-e-lider-em-acesso-nao-autorizado-de-aparelhos-moveis-a-redes-corporativas/>. Acesso em: 27 maio 2012.