UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

MITIGAÇÃO DE RISCOS DE SEGURANÇA DE DISPOSITIVOS ANDROID BASEADA NA MELHORIA DAS DECISÕES DE CONFIGURAÇÃO DO USUÁRIO

THAÍS ANTUNES BIONE

RECIFE

DEZEMBRO / 2015

MITIGAÇÃO DE RISCOS DE SEGURANÇA DE DISPOSITIVOS ANDROID BASEADA NA MELHORIA DAS DECISÕES DE CONFIGURAÇÃO DO USUÁRIO

THAÍS ANTUNES BIONE

MITIGAÇÃO DE RISCOS DE SEGURANÇA DE DISPOSITIVOS ANDROID BASEADA NA MELHORIA DAS DECISÕES DE CONFIGURAÇÃO DO USUÁRIO

Monografia apresentada ao Curso de Bacharelado em Ciência da Computação da Universidade Federal Rural de Pernambuco (UFRPE) como requisito parcial para obtenção do título de Bacharel em Ciência da Computação. Orientador: Prof. Fernando Antonio Aires Lins

BANCA EXAMINADORA

Prof. Dr., Fernando Antonio Aires Lins

DEINFO/UFRPE

Prof. MSc. Francielle Silva dos Santos

DEINFO/UFRPE

Prof. Dra. Jeisa Pereira de Oliveira Domingues

DEINFO/UFRPE

AGRADECIMENTOS

Em primeiro lugar a Deus, por me permitir ter chegado até aqui, e por me dar forças nos momentos em que desistir parecia ser tão mais fácil. Por não ter me deixado de lado mesmo quando não mereci o apoio, e por estar comigo nos meus piores e melhores momentos.

Em segundo, àquela que eu me inspiro e que faz e sempre fez tudo por mim. Obrigada mãe, que também é meu pai. Obrigada por me fazer querer sempre ir em busca dos meus sonhos, e lutar por isso. Obrigada pelo apoio proporcionado quando eu mais precisei, e por toda a compreensão pelos meus momentos de estresse, impaciência e silêncio. Eu te amo, muito.

Agradeço ao meu orientador, professor e amigo Fernando Antonio Aires Lins por toda paciência e companheirismo nessa jornada e em todas durante o curso. Agradeço por cada palavra de incentivo, cada cobrança, e por cada comemoração em conquistas minhas.

Obrigada também aos meus familiares, em especial ao meu avô, que já não se faz presente em matéria entre nós. Obrigada, vovô! Agradecimentos eternos à minha avó Eulina, que desde quando eu era pequena, ensinou-me a importância dos estudos. Obrigada às minhas primas, meus primos, às minhas tias e tios.

Obrigada aos meus amigos e amigas que a vida me presenteou. Às minhas amigas que desde a época do colégio estão ao meu lado, são minhas companheiras das melhores e piores horas. Obrigada por terem me aguentado, por suportarem meu abuso, minha tensão e meu mau humor, de quase sempre. Obrigada por me ouvir, me acalmar e por me ajudar a levantar a cabeça e seguir em frente.

Obrigada mestres pelos ensinamentos e pelo comprometimento, obrigada Sandra pelo apoio e pela ajuda de sempre. Obrigada colegas de curso, alguns mais que colegas, companheiros para toda a vida, em especial a Jamerson, que foi meu braço direito no momento em que mais precisei. Obrigada também a Juliana, Tiago e Guilherme, por terem me dado a oportunidade do meu primeiro e inesquecível estágio, o REDU. Local onde fiz amigos maravilhosos, como Jéssica e Brunno, a quem agradeço por todo apoio de sempre.

RESUMO

Tem-se por riscos de segurança situações que podem levar ao usuário uma maior vulnerabilidade a ataques ~~de~~ por parte de agentes maliciosos. Esses ataques podem ser resultantes de ações a partir do comportamento de usuário, entre elas, decisões de configurações perigosas que podem levar a riscos desnecessários. Portanto, com o intuito de proporcionar ao usuário comum (usuário que não possui um grandes noções de computação e segurança da informação) um maior conhecimento para o auxiliar em decisões de configuração, este trabalho objetiva a elaboração de uma estratégia. Esta estratégia é composta por uma cartilha, onde são descritas sugestões de boas práticas que auxiliarão o usuário no que se trata de reduzir a exposição de seus dispositivos aos mais comuns e reincidentes tipos de ataque, e por uma aplicação que provê suporte tecnológico a boa parte das práticas sugeridas na cartilha. A fim de avaliar boas práticas para contemplá-las na cartilha, foram realizadas entrevistas com questões direcionadas às tomadas de decisão pelo usuário. As entrevistas concluíram que, embora aproximadamente 67% dos entrevistados tenha afirmado se preocupar com a segurança das informações de seu dispositivo, 74% possui um dos modos de controle de acesso mais fáceis de serem descobertos, o desenho padrão. Essas mesmas entrevistas revelaram que apenas 20% dos entrevistados leem permissões as quais os aplicativos a serem instalados requerem acesso.

Os resultados obtidos a partir das entrevistas serviram como base para o desenvolvimento das boas práticas sugeridas na cartilha citada acima. As sugestões se referem a comportamentos que podem ser evitados/tomados pelo usuário, a partir da gestão da configuração. Para cada tópico foi esclarecido o motivo da necessidade de o mesmo se fazer presente no documento como medida preventiva a respeito da segurança da informação e/ou do dispositivo. Para avaliar a aplicação implementada, foram realizados testes em dispositivos para verificar a presença de vulnerabilidades buscadas pela mesma. Entre outros resultados verificou-se que, por exemplo, dos aparelhos testados, 86.7% estavam com o a *Wi-Fi* ativa durante o teste e apenas 67% estavam conectados à alguma rede. Portanto, pode-se afirmar que a estratégia apresenta uma contribuição importante para a sociedade, principalmente para os usuários comuns, que não possuem uma grande noção sobre computação e segurança da informação.

Palavras-chave: Segurança em dispositivos móveis, Android, Configurações de usuário, Interfaces de conexão sem fio.

ABSTRACT

It has been a security risk situations that can lead to the user more vulnerable to security attacks by malicious agents. These attacks can result from actions from the user behavior, among them dangerous configuration decisions that can lead to unnecessary risks. Therefore, in order to provide the regular user (user who does not have great notions of computing and information security) greater knowledge to assist him in configurations decisions, this work aims to draw up a strategy. This strategy consists of a primer, which are described suggestions of good practice that will help the users when it comes to reducing the exposure of their devices to the most common and recurrent types of attacks, and an application that provides technological support for the most of the practices suggested in the booklet. In order to assess best practices to address those in the booklet, questions interviews were conducted with the user-directed decision-making. The interviews concluded that although approximately 67% of interviewed have stated to worry about the safety of their device information, 74% has one of the easiest access control modes to be discovered, the standard design. These same interviews revealed that only 20% of interviewed read permissions which applications to install require access. The results obtained from the interviews served as the basis for the development of good practices that was suggested in the booklet mentioned above. The suggestions relate to behaviors that can be avoided / taken by the user, from the configuration management. For each topic has clarified the reason for the need for it to be present in the document as a preventive measure regarding the safety information and / or device. To evaluate the application implemented in, devices tests were performed to verify the presence of the same vulnerabilities sought. Among other results it found that, for example, the devices tested, 86.7% were active with the WiFi during the test and only 67% were connected to any network. Therefore, it can be said that the strategy is a valuable contribution to society, especially for regular users, who do not have a great sense of computing and information security.

Key words: Security, Mobile Computing, Android.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS, SIGLAS E SÍMBOLOS

APP – *Application*, termo em inglês para Aplicação.

BPMN - *Business Process Model and Notation*, termo em inglês para Notação de Modelagem de Processos de Negócio.

CAIS - Centro de Atendimento e Incidentes.

CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.

CID - Confidencialidade, Integridade e Disponibilidade.

GPS – *Global Positioning System*, termo em inglês para Sistema de Posicionamento Global.

ID - *Identity Document*, termo em inglês para Identidade.

NET – *Network*, termo em inglês para Rede.

PHA – *Potentially Harmful Application*, termo em inglês para Aplicações Potencialmente Prejudiciais.

PIN – *Personal Identification Number*, termo em inglês para Número de Identificação Pessoal.

RNP - Rede Nacional de Ensino e Pesquisa.

SBSeg – Simpósio Brasileiro em Segurança da Informação e Sistemas Computacionais.

SMS – *Short Message Service*, termo em inglês para Serviço de Mensagem Curta.

SSL – *Secure Socket Layer*, termo em inglês para Camada de Soquete Segura.

TLS – *Transport Layer Security*, termo em inglês para Camada de Transporte Segura.

UFRPE - Universidade Federal Rural de Pernambuco.

WAP – *Wireless Application Protocol*, termo em inglês para Protocolo para Aplicações Sem Fio.

WEB – *World Wide Web,* termo em inglês para Rede Mundial de Computadores.

SUMÁRIO

1 INTRODUÇÃO

Com a evolução da tecnologia móvel e com o aumento da facilidade a essa tecnologia, o consumo de dispositivos móveis tem aumentado em grande escala. Segundo o estudo divulgado pela consultoria Gartner, líder mundial em pesquisa e aconselhamento sobre tecnologia, mais de 112 milhões de dispositivos conectados, entre *tablets, hotsposts* móveis e computadores pessoais com modem celulares incorporados serão vendidos durante o ano de 2015. Ainda de acordo com a Gartner, em 2016, serão 160 milhões, e existe potencial para 600 milhões de unidades até 2019 (AURICCHIO J., 2015).

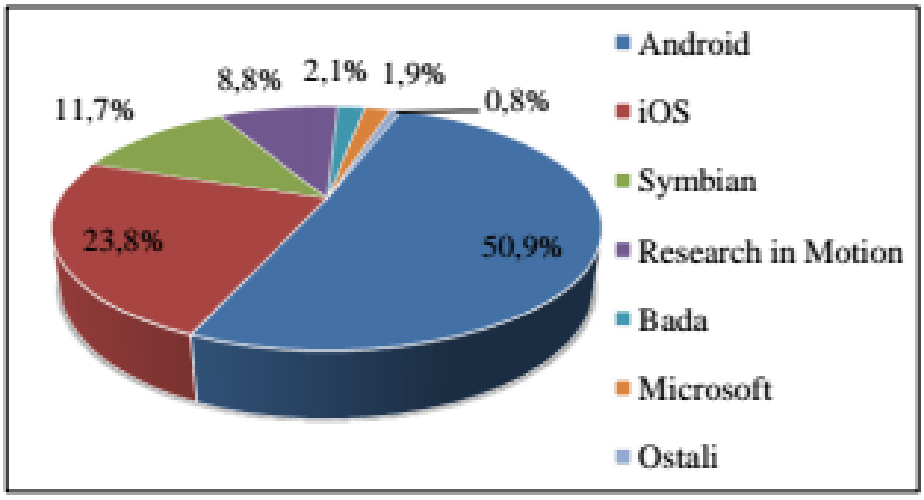
Os principais dispositivos que atendem à tecnologia em estudo, dispositivos móveis com o sistema operacional Android, são os *tablets e smartphones.* Quando inseridos no mercado, esses dispositivos foram a princípio utilizados com finalidade fundamentalmente pessoal. Porém, com o passar do tempo, começou a ser evidenciada a execução desses dispositivos para atividades profissionais. Uma pesquisa realizada pela *Accenture*, empresa de tecnologia, afirma que 61% dos brasileiros que possuem *tablets*, utilizam esse dispositivo para executar fins profissionais (VIASOFT, 2012), como também, para a realização de tarefas antes executadas exclusivamente através de computadores pessoais com acesso à internet. O Brasil, com 70 milhões de unidades, é o quarto país do mundo em *smartphone* (SWISHER, 2012). Esse avanço resulta, inevitavelmente, no incremento de possíveis ataques/riscos relacionados a esses dispositivos. Agentes maliciosos são atraídos a proporcionar situações que levam esses dispositivos móveis a sofrerem ameaças de segurança uma vez que houve também o aumento do número de serviços e aplicações, volume de informações financeiras, particulares e corporativas trafegadas.

Diante desse expressivo crescimento do número de dispositivos móveis, destaca-se a preferência por dispositivos com sistema operacional Android (PERAKOVIĆ; HUSNJAK; REMENAR, 2012).

A Figura 1 ilustra a predominância do uso do sistema operacional Android em comparação a outros sistemas como iOS, da Apple e o Symbian, da Nokia. De acordo com a figura, o Android possui 50,9 % dos 100% totais dos entrevistados, fator que demanda uma maior preocupação em relação à segurança, pois, devido a essa

preferência pela plataforma, usuários maliciosos têm cada vez mais optado por ataques à mesma.

Figura 1. Sistemas Operacionais Para Dispositivos Móveis Mais Utilizados.



Fonte: (PERAKOVIĆ; HUSNJAK; REMENAR, 2012).

O aumento do poder de computação, a grande conectividade e o expressivo aumento da variedade de serviços e aplicativos disponíveis nos dispositivos móveis com o sistema operacional Android colocam os *smartphones* e *tablets* em evidência como alvos de ataques de segurança (BRAGA *et al.*, 2012). Entende-se por ameaça de segurança aquelas que podem comprometer a confidencialidade, propriedade que limita o acesso à informação apenas às entidades autorizadas pelo proprietário da informação, integridade, propriedade que garante que a informação possuirá as características originais estabelecidas pelo proprietário da informação, e disponibilidade, propriedade que garante que a informação estará sempre disponível para o uso legítimo (PAULO; KOVACS; MONTEIRO, 2006).

A segurança do Android pode ser otimizada através do uso cauteloso por parte de seus usuários. Serviços de permissão e controle de acesso, que são de responsabilidade do usuário, podem introduzir ao dispositivo vários riscos de segurança, caso mal utilizados. Como exemplo, há a ativação de funções de interface de conexão seja via *bluetooth* ou *wi-fi*, pois podem possibilitar a invasão de dispositivos sem que haja permissão do proprietário, a instalação de *malwares* a partir de aplicativos de origem desconhecida e acesso a *sites* desconhecidos através do navegador do dispositivo.

O estudo do tema proposto por este trabalho teve início a partir ~~de uma~~ experiência de um projeto de extensão realizado na UFRPE (Universidade Federal Rural de Pernambuco). O projeto teve como título Desenvolvimento de Políticas de Segurança Para Uso de Dispositivos Móveis. Seu início se deu a partir da percepção de que o uso de *tablets* e *smartphones* tornou-se uma realidade no cotidiano da sociedade em geral, e da necessidade de haver um estudo pela segurança desses dispositivos (BIONE, T.A., LINS, F.A.A., 2013), (BIONE, T.A., LINS, F.A.A., 2014), (BIONE, T.A., LINS, F.A.A., 2015).

Uma das questões mais relevantes é a segurança dos dados do proprietário do dispositivo. Dessa forma, medidas preventivas foram buscadas com a finalidade de minimizar o risco de um ataque de segurança a partir de vulnerabilidades existentes e provenientes do mal uso, a partir de tomadas de decisões do usuário.

O projeto visou a elaboração de um conjunto de políticas de segurança a serem seguidas por usuários do sistema operacional Android, com o intuito de reduzir a possibilidade de ocorrência de problemas de segurança. Para tal, duas vertentes foram seguidas:

1) Pesquisa e desenvolvimento de políticas de segurança para uso de dispositivos móveis, baseadas no perfil do usuário;

2) Disseminação e apresentação das políticas desenvolvidas para a sociedade.

Essas vertentes foram obtidas a partir da realização de quatro fases, nas quais o projeto foi realizado. Na primeira fase foi realizado o estudo aprofundado sobre tecnologias e documentos existentes, a partir do levantamento bibliográfico sobre segurança em computação móvel. Na segunda fase optou-se por estudar políticas de segurança para mitigar possíveis riscos de segurança ao se utilizar um dispositivo com o sistema operacional Android. Foram realizadas pesquisas em artigos, livros e outras bibliografias pertinentes. Buscou-se por segurança com ênfase no usuário final, pois, o Android permite ao usuário a tomada de decisões e gerência de configurações que quando ~~má~~ definidas, podem levar a ataques de segurança. Na terceira etapa foram desenvolvidas as políticas de segurança a partir da busca pelos mais reincidentes riscos/problemas provenientes dessa má gestão/configuração, e suas principais soluções preventivas. E por fim a quarta etapa, que se caracterizou pela identificação dos riscos e suas soluções além da documentação, em forma de uma cartilha, (pequeno documentos

com o intuito de ensinar acerca de um assunto, com boas práticas para usuários de dispositivos Android, e da apresentação dessas informações à sociedade.

Embora se saiba da existência de cartilhas ~~já existentes~~ sobre segurança de dispositivos móveis, coube a este trabalho a elaboração de uma nova cartilha pelo fato de as já existentes terem sido publicadas em 2012 e não serem direcionadas para dispositivos móveis com sistema operacional Android. Buscou-se, então, o desenvolvimento de uma cartilha mais atualizada a partir de estudos em fontes mais ~~atuais~~, além de direcionada aos dispositivos com o sistema operacional Android. Adicionou-se, por exemplo, a sugestão de ativar a função *Verify Apps*, que é responsável por buscar vulnerabilidades nos aplicativos instalados. A ativação da função não foi sugerida nas cartilhas estudadas. Em paralelo a essa cartilha, deu-se início a implementação de uma aplicação apta a, junto ao usuário, verificar se as soluções/configurações sugeridas estão sendo aplicadas.

Portanto, com a finalidade de auxiliar os usuários finais para uso menos vulnerável a ataques, este documento objetiva a elaboração de uma estratégia integrada, composta por uma cartilha que contempla as práticas mais comuns para prover o uso mais cauteloso dos dispositivos móveis a partir da configuração do aparelho, e por uma aplicação desenvolvida para dar suporte ao uso dessa cartilha.

1.1 OBJETIVOS GERAIS E ESPECÍFICOS

O objetivo principal deste trabalho é a proposta da estratégia integrada, composta por uma cartilha e uma aplicação, para suporte a melhoria das decisões de configuração do usuário de dispositivos móveis Android.

A nível de objetivos específicos, tem-se os pontos descritos a seguir.

- **Investigar os mais reincidentes problemas/riscos de segurança em dispositivos móveis**. Devido à grande capacidade de armazenamento de dados pessoais, ao grande poder de computação e à fácil aquisição, o uso de dispositivos móveis aumentou. Esse fator atraiu usuários maliciosos com o intuito de interceptar esses dados, independente da finalidade. Portanto, é necessária a investigação das maiores incidências dos ataques, suas formas e tipos para que posteriormente seja possível a elaboração da solução dessas vulnerabilidades identificadas;

- **Investigar as principais soluções para os mais reincidentes problemas/riscos de segurança nos dispositivos móveis**. Além de identificar as vulnerabilidades que levam aos principais ataques idealizados pelos usuários maliciosos, é objetivo deste trabalho a busca de soluções capazes de proporcionar ao usuário um serviço mais seguro e menos propício a ataques invasivos. Portanto, foram analisados os maiores problemas/riscos de segurança e listadas as principais soluções que vão ao encontro da mitigação dos possíveis meios de ataques identificados;
- **Elaboração de uma cartilha com os mais recorrentes problemas/riscos de segurança e suas respectivas soluções a partir das configurações de usuário com foco em segurança.** O Android é um sistema operacional que permite que o usuário esteja apto a tomar decisões e optar por configurações que, quando mal tomadas e configuradas, podem deixar em risco o dispositivo móvel em questão. Portanto, teve-se a ideia de listar em um único documento as principais sugestões para tomadas de decisões a partir da configuração do usuário, com a finalidade de prover uma experiência mais segura ao configurar seu dispositivo móvel. Neste contexto, a ideia é produzir algo que fique à disposição de todos da comunidade e seja de fácil acesso e entendimento. Para tal, foi construída uma cartilha autoexplicativa;
- **Desenvolvimento de aplicação em Android como suporte à cartilha, que tem o objetivo de auxiliar o usuário a verificar se itens descritos na cartilha estão sendo realizados.** Além da percepção da necessidade da cartilha e da elaboração da mesma, surgiu a ideia da implementação de uma aplicação que pudesse ser capaz de auxiliar o usuário a seguir as sugestões da cartilha. Portanto, foi desenvolvida uma aplicação capaz de verificar se alguma das más configurações do usuário estão presentes no aparelho, e de retornar aos usuários vulnerabilidades encontradas.

1.2 ESTRUTURA DO TRABALHO

O capítulo 2 aborda alguns conceitos básicos que serão utilizados ao longo do trabalho. Neste capítulo, estarão presentes conceitos relacionados à plataforma Android, tecnologia móvel, e assuntos que concernem ao trabalho em si, como segurança da informação.

O capítulo 3 aborda os mais relevantes trabalhos relacionados no contexto da temática abordada neste documento. Neste capítulo serão apresentados os principais referenciais teóricos para o embasamento da cartilha, e será feita uma visão comparativa entre os elementos citados e o trabalho desenvolvido.

O capítulo 4 aborda a cartilha proposta através da apresentação de cada sugestão contida na mesma. Neste mesmo capítulo é apresentada a aplicação implementada, a modelagem para a construção da mesma e a identificação de seus casos de uso.

No capítulo 5 são apresentadas as avaliações. ~~Serão~~ exibidos a entrevistas e os seus resultados. Há também uma comparação entre a cartilha construída e uma cartilha para dispositivos móveis já existente e a avaliação dos itens sugeridos pela mesma, a partir de testes com a aplicação e dispositivos do usuário.

No capítulo 6 estão presentes as considerações finais, como também, a apresentação dos trabalhos futuros.

2 CONCEITOS BÁSICOS

Neste capítulo serão apresentados os principais conceitos necessários para o entendimento deste trabalho. Serão abordados assuntos desde uma breve introdução aos dispositivos móveis e visão geral do sistema operacional Android até à segurança da informação.

2.1 DISPOSITIVOS MÓVEIS

Entende-se por dispositivos móveis qualquer equipamento eletrônico com atribuições de mobilidade como: *notebooks*, *smartphones*, *tablets*, entre outros.

Os dispositivos móveis em sua maioria são utilizados para os mais diversos fins, desde diversão até o trabalho. Possuem um sistema operacional instalado, que podem variar de acordo com o fabricante do aparelho. Esse sistema operacional é desenvolvido especificamente para o dispositivo móvel, de forma a considerar suas especificidades, como bateria limitada, tamanho reduzido e capacidade de processamento/armazenamento mais limitados em relação aos tradicionais *desktops*.

BlackBerry OS, Android, IOS e Windows Phone estão entre os principais SOs móveis disponíveis no mercado. Destaca-se a preferência por dispositivos com sistema operacional Android (PERAKOVIĆ; HUSNJAK; REMENAR, 2012). Por este motivo, o sistema operacional Android será abordado na próxima seção.

2.2 SISTEMA OPERACIONAL ANDROID

Conforme visto na seção anterior, há uma diversidade de sistemas operacionais a serem escolhidos pelo usuário, de acordo com a marca e fabricante do seu dispositivo móvel. No desenvolvimento deste trabalho optou-se por enfatizar dispositivos móveis com sistema operacional Android, portanto, cabe a esta sessão uma breve introdução à essa plataforma.

2.2.1 Introdução ao Sistema Operacional Android

O Android foi desenvolvido pela *Open Handset Alliance*, uma parceria entre diversas empresas, incluindo a Google, e é um sistema que opera em dispositivos móveis como *smartphones*, *tablets*, *notebooks* e relógios.

Desde seu lançamento em 2008, o Android tem sido um dos sistemas operacionais para dispositivos móveis mais vendidos. Três das principais razões que o caracteriza como uma das plataformas mais vulneráveis são: A abertura da plataforma, o que significa que qualquer pesquisador e desenvolvedor do mundo pode ter acesso ao seu código fonte, a revisão limitada de aplicativos na *Google Play Store*, e a compatibilidade do dispositivo com aplicativos de fornecedores de terceiros. A cada dia, mais de um milhão de novos dispositivos móveis com o sistema operacional Android são ativos (MOHINI; KUMAR; NITESH, 2013). A razão pela qual o Android é a plataforma para dispositivos móveis mais utilizada pode ser justificada através da análise dos seguintes pontos:

- **O Android é um sistema baseado no código Linux.** O Linux possui licença aberta, e com isso permite que vários desenvolvedores possam contribuir para o sistema;
- **Possui uma grande variedade de dispositivos.** Por ser adotado por uma grande quantidade de fabricantes (Motorola, LG, Samsung, CCE, HTC, HUAWEY, entre outros), possui liberdade de customização quando permite que o usuário não fique preso à interface padrão do sistema;
- **Possui grande variedade de aplicativos.** Conta com mais de um milhão de aplicações em sua loja oficial, a Google Play;
- **Possui maior integração com os serviços do Google.** Android é uma plataforma que tem o Google como um de seus desenvolvedores**.**

2.2.2 Características

O Android é um sistema operacional que dá suporte a vários tipos de *hardware,* além de possuir suporte adicional à hardware, como por exemplo câmera de vídeo, tela sensível ao toque, GPS e aceleração de gráfico 3D (BRAGA *et al.*, 2012).

O Android possui ainda uma maior integração com os serviços do Google, como o GMAIL, *Google Calendar* e contatos da WEB (ENCK *et al.*, 2011). Além da grande flexibilide por parte do usuário ao instalar aplicativos, que podem ser adquiridos através da loja oficial da plataforma, a *Google Play,* ou a partir de lojas externas.

2.3 SEGURANÇA DA INFORMAÇÃO

O termo Segurança da Informação se refere à proteção existente sobre as informações. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para seu proprietário (REIS, 2011).

As informações podem estar guardadas para uso restrito ou estarem expostas ao público para consulta ou aquisição. Podem ser estabelecidas métricas para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal-intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação (RODRIGUES; CARVALHO, 2012).

De acordo com (STALLINGS, W.; BROWN L, 2011) há três conceitos que incorporam os objetivos de segurança fundamentais para dados e informações, bem como para serviços de computação. Esses conceitos formam a tríade CID (Confidencialidade, Integridade e Disponibilidade).

As definições desses principais atributos ainda segundo (STALLINGS, W.; BROWN L, 2011), são:

- Confidencialidade – Preservar restrições autorizadas ao acesso e revelação de informações, incluindo meios para proteger a privacidade pessoal e as informações proprietárias. Uma perda de confidencialidade consiste na revelação não autorizada de informações.
- Integridade – Defender contra a modificação ou destruição imprópria de informações. Uma perda de integridade consiste na modificação ou destruição não autorizada de informações.
- Disponibilidade – Assegurar que o acesso e o uso das informações seja confiável e realizado no tempo adequado. Uma perda de disponibilidade consiste na disrupção do acesso ou da utilização de informações de um sistema de informação.

2.3.1 Ameaça, Vulnerabilidade e Riscos

Ameaça é o termo utilizado para representar situações que podem pôr em risco a tríade Confidencialidade, Integridade e Disponibilidade, principais atributos integrantes da segurança da informação.

Vulnerabilidades são representadas pelas falhas de segurança que podem ser exploradas, sejam elas intencionalmente ou não, resultando assim na quebra de um ou mais dos princípios da segurança da informação. Ao terem sido identificadas as vulnerabilidades, será possível dimensionar os riscos aos quais o ambiente está exposto e assim definir medidas de segurança apropriadas para sua correção (CAMPOS, 2007).

Entende-se como riscos, situações que expõem às informações a sofrerem danos e perdas.

Como exemplos de ameaças comuns em *smartphones* podem-se citar (NAMESTNIKOV; MASLENNIKOV, 2012):

- ***Malwares***. *Softwares* maliciosos encontrados nas lojas oficiais e extraoficiais de aplicações;
- ***Botnets.*** Redes controladas por criminosos que comandam máquinas infectadas com a intenção de tomar controle do dispositivo para realizar ataques;
- **Roubo de dados dos dispositivos móveis.** O agente do ataque tem o intuito de tomar posse dos dados do usuário, seja para conseguir dinheiro com a recuperação do mesmo pelo próprio usuário, ou ainda para utilizá-los;
- **Rastreamento de pessoas e serviços de geolocalização**. Quando o atacante tem o intuito de obter acesso à localização do usuário, ou ainda, prever onde ele pode estar, de acordo com os perfis criados da análise de várias localizações disponíveis pelo seu dispositivo.

3 TRABALHOS RELACIONADOS

Para a escrita deste trabalho realizou-se pesquisas nos mais diversos tipos de fontes. Buscou-se por artigos científicos, estudos acadêmicos e também livros técnicos, com a finalidade de obter informações em torno do assunto: vulnerabilidade em dispositivos móveis a partir da gestão/configuração de tomadas de decisões do usuário comum. Porém, devido à especificação da problemática em análise, as buscas nas fontes citadas não retornaram informações suficientes, o que acarretou na necessidade da utilização de *blogs* e *sites* de instituições especializadas em tecnologia da informação, ou ainda de empresas voltadas à área de segurança da informação. Essas fontes alternativas podem ser exemplificadas por: (GOOGLE, 2014), (VIASOFT, 2012), (NAMESTNIKOV; MASLENNIKOV, 2012).

A nível de referencial para embasamento teórico, foram selecionadas três diferentes fontes. Essa escolha deu-se pelo fato de as três terem proporcionado ao desenvolvimento deste trabalho uma maior quantidade de informações relevantes sobre o tema em discussão (segurança em Android). Essas fontes serão abordadas em tópicos a seguir.

3.1 RELATÓRIO DA GOOGLE SOBRE A SEGURANÇA DO ANDROID (GOOGLE, 2014)

Essa referência foi escolhida por ser uma das bibliografias mais relevantes dentre as mais atuais encontradas. O documento tem um foco maior no que fala a respeito dos dispositivos que sofreram o ataque de segurança a partir da instalação das aplicações. Trata-se do primeiro relatório oficial da Google sobre a segurança em dispositivos móveis com o sistema operacional Android, através da análise de dados coletados durante o ano de 2014. Todos os registros a seguir são resultados dessa análise.

Segundo o relatório, existem duas principais formas de se obter um aplicativo:

1) **Através da loja oficial da Android, a *Google Play Store.*** Os usuários direcionam-se à loja do Android através do aplicativo que já vem instalado de fábrica no celular, ou dirigem-se ao site oficial da loja e baixam a aplicação desejada;
2) **Através de fornecedores externos à *Google Play Store.*** Os usuários dirigem-se a outras fontes virtuais e baixam a aplicação desejada.

Em 2014 menos de 1% de todos os dispositivos teve um *PHA* (*Potentially Harmful Application*) instalada. Menos de 0,15% desses *PHA* foram instalados através da loja oficial do Android (GOOGLE, 2014). Existem atualmente dos tipos de segurança fornecidos pelo *Google Play* para todos os usuários do Android:

- **Proteção dentro da própria *Google Play*.** *R*efere-se à verificação do aplicativo para verificar se o mesmo se trata de uma *PHA* (*Potentially Harmful Application*);
- **Proteção para aplicações fora da *Google Play.*** Refere-se ao serviço de *Verify Apps* (Verificação de Aplicativos), explicado logo abaixo.

Verify Apps é um serviço inserido desde 2012 que oferece proteção contra aplicativos obtidos fora da loja oficial, a Google Play. Sua ativação/inativação pode ser realizada pelo usuário ao acessar o menu de configurações do aparelho. A ferramenta permanece em execução em segundo plano no aparelho do usuário, sempre atenta às aplicações. O serviço vem fornecendo dados valiosos para entender o comportamento de certos recursos ilegais utilizados para a captura de informação do aparelho, tais como *spyware* (qualquer aplicação para capturar informações do dispositivo e fornecê-las para partições terceiras sem que haja conhecimento do proprietário das mesmas), *ransonware* (tipo de software malicioso que restringe o acesso ao sistema infectado e cobra um valor para que o acesso possa ser reestabelecido) e fraudes de WAP (*Wireless Application Protocol*, do português: Protocolo de Redes sem fio) e SMS (*Short Message Service*, do português: Serviço de Mensagem Curta).

Por exemplo, na semana anterior a 1º de novembro de 2014, o *Verify Apps* escaneou mais de 200 milhões de dispositivos apenas em um dia. No entanto, a ferramenta, por razões de privacidade, coleta do aparelho apenas os dados necessários para prover e melhorar a segurança, deixando de lado qualquer informação pessoal, além de não registrar as coordenadas geográficas da localização do dispositivo.

Como resposta ao resultado do serviço de *Verify Apps*, a equipe de segurança do Android desenvolveu 79 *patches* (programas de computador criado para atualizar ou corrigir um *software*). Desses *patches*, 41 foram classificados como moderados, 30 como altos e 8 como baixos. Ainda segundo o relatório escrito pela Google, não houve vulnerabilidade crítica encontrada em 2014.

O relatório do Google descreve também uma forma interessante de classificar riscos de segurança. Esta forma assim descrita:

- **Crítica** → Exploração ativa através da execução remota de permissões de nível de proteção do Android, ou através da utilização normal do dispositivo;
- **Alta** → Execução remota com habilidade de rodar as permissões de nível de proteção do Android. Acesso remoto a dados protegidos;
- **Moderada** →O acesso local aos dados sensíveis, sem privilégio apropriado. Negação de serviço que torna o dispositivo inutilizável. Eleva nível de permissão do usuário. Torna-o como *root* (usuário administrativo) sem que seja necessária uma autorização;
- **Baixa** → Acesso local não autorizado a dados que não são considerados sensíveis. Negação de serviço que pode ser interrompido por usuário normal, como reinicialização do sistema ou a remoção do aplicativo. Ou ainda, a violação limitada do modelo de segurança do Android.

Em caso de um aplicativo ser classificado como potencialmente prejudicial, além de exibir um aviso ao usuário, o *Verify Apps* bloqueia a instalação ou permite ao usuário continuar. Entende-se por potencialmente prejudicial um aplicativo que após instalado, pode fornecer riscos de segurança ao dispositivo e seu usuário.

Porém, há usuários que cancelam a proteção dos recursos de segurança do Android e, por exemplo, instalam esses aplicativos suspeitos em modo *root*, modo no qual o usuário possui total permissão sobre o sistema por meio de acesso administrativo.

Recentemente, antes de serem disponibilizados para a *Google Play*, os aplicativos começaram a passar por um processo de revisão de segurança para garantir que estão em conformidade com a política de segurança adotada pelo sistema, na qual, não se encaixam *PHA*. Essa verificação ocorre através da aprendizagem de máquinas que analisam dados, nós ativos e gráficos de relacionamento para construírem sistemas de alta precisão com a finalidade de detectar falhas de segurança. Essas máquinas fazem conexões e verificam padrões que os seres humanos não seriam capazes em tempo hábil.

Por fim, é relevante ressaltar que embora esta fonte tenha sido relevante ao trabalho, trata-se de um relatório feito por uma empresa independente, a Google, a respeito de um produto que a própria Google é *sponsor*. Os dados apresentados

favorecem a empresa e afirmam que a segurança do Android passou por um processo de melhoria, reduzindo a quantidade de aplicações com código malicioso. Seria importante que um agente externo às duas empresas realizasse essa pesquisa, e produzisse um novo relatório.

3.2 INTRODUÇÃO À SEGURANÇA DE DISPOSITIVOS MÓVEIS MODERNOS – UM CASO DE USO EM ANDROID (BRAGA *ET AL.*, 2012).

Este documento é foi apresentado e debatido durante os minicursos do XX Simpósio Brasileiro em Segurança da Informação e Sistemas Computacionais, SBSeg. Considerando o objetivo deste trabalho, optou-se por esse documento pelo fato de o mesmo abordar aspectos de segurança da informação relacionados aos dispositivos móveis modernos, exibindo ameaças, vulnerabilidades na plataforma Android.

Os aspectos de segurança relacionados aos dispositivos móveis são abordados de acordo com três aspectos inter-relacionados. O primeiro é a constatação de que os dispositivos móveis representarão a próxima forma de proliferação de *software* malicioso. Este fato foi evidenciado pelo grande aumento da quantidade de artefatos maliciosos voltados à plataforma Android, pelo fato da grande representação no mercado desta plataforma em relação às outras plataformas de dispositivos móveis. O segundo é chamado de consumerização, onde as tecnologias novas surgirão voltadas para usuários finais e apenas posteriormente para o segmento corporativo. Deste modo, passam a utilizá-los de modo intenso não apenas em atividades pessoais, mas também profissionais, o que pode por em risco informações importantes da corporação. O terceiro aspecto é um desdobramento dos anteriores, em que, em um ambiente com plataforma para dispositivos móveis, muitos dos controles de segurança tradicionais, comumente aplicados sobre *desktops* e outros ativos da infraestrutura, tornam-se ineficazes. Como por exemplo, os softwares maliciosos, pois nesses ambientes móveis sua proliferação não se dá apenas por transferências diretas entre dispositivos. Algumas proliferações dão-se através da instalação de aplicativos a partir da própria loja oficial ou de lojas provenientes de sites terceiros. Além disso, há ainda a utilização de *botnets* (grupos de dispositivos controlados remotamente por um atacante) em *smartphones* para realização de ataques maciços sincronizados e outras fraudes coordenadas, incluindo ataques potenciais à rede de telecomunicações.

O Android é uma plataforma *mobile open source*, cuja concepção inicial foi do Google, e posteriormente passou para a *Open Handset Alliance*. A plataforma Android

foi concebida de modo que sua arquitetura de segurança permite que controles sejam aplicados de forma que exista o confinamento de aplicações através do esquema de permissões. Dispositivos móveis com o sistema operacional Android são configurados de modo que o usuário não possua total permissão sobre o sistema por meio de acesso administrativo (*root*). O termo *rooting* equivale a obter permissões de acesso às permissões da conta. As motivações para a habilitação de tal acesso são várias, como por exemplo: instalação de versões modificadas do Android; uso de temas personalizados; backup de todos os dados; e também, ativar funcionalidades que foram bloqueadas por operadoras.

No Android é possível definir um controle de acesso ao sistema, para isso são definidos 4 modos com diferentes níveis de segurança.

• **Reconhecimento Facial**: é um modo de segurança considerado inseguro. Tem-se registros de ataques nos quais esse controle foi quebrado com foto sendo apresentada ao sensor. Uma foto pode ser facilmente obtida através de outro dispositivos com câmera ou então através das redes sociais.

• **Padrão de desenho:** Desenha-se um padrão na tela ligando pontos em um campo. Considerando um campo 3x3, este modo pode ser representado por uma que uma senha de nove números, os quais não podem ser repetidos. Algo que pode ser quebrado em um ataque de força bruta. Pode-se ainda observar os manchas que o dedo deixa na tela do dispositivo, obtendo assim o rastro com o desenho padrão.

• **PIN**: Trata-se do desbloqueio através de uma senha numérica. Por mais forte que seja a senha, o fato de ser composta apenas por caracteres numéricos limita sua segurança.

• **Senha:** Modo que possibilita o uso de letras, números e símbolos. Devido ao domínio mais extenso de possibilidades, tal escolha é a mais segura.

Para aumentar a segurança em dispositivos móveis com o Android, a partir da versão 3.0 foi implementada a funcionalidade de encriptação de disco/partição de dados. Pois, os controles de segurança aplicados pelo sistema operacional não são suficientes para a proteção dos dados. Logo, um usuário malicioso com acesso físico ao aparelho poderia obter todas as informações nele armazenadas.

O modelo de confinamento do Android é um modelo no qual o Android trata cada aplicativo como um usuário, mapeando um ID exclusivo em tempo de instalação. Para cada aplicativo, cria-se um diretório no sistema de arquivos onde todos os arquivos associados serão armazenados. Apenas o ID do aplicativo possui total acesso a esse

diretório, o grupo ao qual pertence e os outros não possuem qualquer permissão de acesso. Esse controle impossibilita o acesso por parte de aplicativos maliciosos a recursos protegidos do sistema ou de outros aplicativos. O ponto positivo deste modelo é que, caso uma vulnerabilidade seja explorada em um aplicativo, o código malicioso injetado permanecerá restrito às permissões da aplicações em questão, não sendo possível o acesso a outros recursos.

A instalação de aplicativos no Android ocorre por meio de lojas virtuais. A loja oficial do Android é a Google *Play*, onde os aplicativos não passavam por nenhum processo de avaliação, até que em 2012 foi apresentada uma solução para avaliar as aplicações. A essa solução denominou-se *Bouncer*. Trata-se de uma simulação do ambiente de execução do Android e execução de um o aplicativo a fim de monitorar seu comportamento e identificar funcionalidades potencialmente maliciosas. Porém, o Android permite a utilização de outras lojas de aplicativos que não são oficiais. A maioria dos *malwares* para a plataforma Android geralmente são encontrados em outras lojas que não a loja oficial [Six 2012].

Os aplicativos para dispositivos móveis manipulam diversas informações dos usuários, tais como contatos, histórico de mensagens e ligações, *e-mails*, documentos diversos, mídias, informações de localização, credenciais de acesso e inclusive informações financeiras. A exposição dessas informações pode causar danos ao usuário, aumentando os riscos associados a estes aplicativos. A ameaça de maior probabilidade de ocorrência é o extravio do dispositivo, que possui um grande risco quando em conjunto com a injeção de código malicioso.

Para se proteger de possíveis ataques que exploram vulnerabilidades, algumas medidas devem ser tomadas pelo proprietário do dispositivo, a fim de se obter um maior nível de segurança. Essas medidas têm uma maior relevância quando tomadas em relação às permissões administrativas. Existem várias opções que se encontram ativadas por padrão no dispositivo, ou ainda que são ativas pelo usuário, mas depois não são desativadas. Algumas delas, enquanto não estão sendo utilizadas, ou quando são mal definidas pelo usuário, podem servir de entrada para possíveis ataques de vulnerabilidades, principalmente por meio de *softwares* maliciosos.

Ainda segundo os autores do minicurso, (BRAGA *ET AL.*, 2012), tem-se como recomendações de segurança a nível do usuário:

Atenção à instalação de aplicativos a partir de fontes desconhecidas: A instalação de aplicativos provenientes de lojas de terceiros abre uma maior probabilidade de entrada para aplicativos maliciosos no dispositivo. Um atacante pode modificar um aplicativo seguro, transformando-o em um software malicioso. Logo, o mesmo poderá ser baixado e executado pelo usuário, ativando suas funções maliciosas.

Bloqueio de tela: Recomenda-se que se utilize o controle por senha de no mínimo 8 caracteres, incluindo caracteres alfabéticos maiúsculos e minúsculos, caracteres numéricos e símbolos, para dificultar o acerto a partir de tentativas e erro. Não se aconselha o uso de palavras comuns ou de dados pessoais.

Encriptação de disco: O ideal é ativá-la, caso haja a opção, para se manter os dados seguros mesmo contra roubo e extravio do dispositivo móvel. É importante definir uma senha forte para a proteção desses dados, caso contrário um atacante poderá facilmente obtê-los por meio de um ataque de força bruta.

***Bluetooth*:** Deixar o *bluetooth* ativado abre mais uma porta para possíveis ataques. A recomendação é que se ative apenas pelo tempo necessário para a realização da atividade pretendida.

Formatação Remota: Nos dispositivos em que a opção estiver disponível, é uma boa precaução a se utilizar, caso o dispositivo seja perdido, seja por roubo ou por extravio. Pois, será possível apagar seus dados remotamente, protegendo-se assim do roubo de informações.

GPS: Deixar o GPS desligado por padrão, e tomar cuidado com opções de aplicativos permitindo que seja monitorada a sua localização. É possível se prever onde um usuário estará de acordo com o perfil criado da análise de várias localizações disponíveis pelo seu dispositivo [Malm e Osborn 2012].

Permissões: É muito comum não se ler quais as permissões que um aplicativo solicita ao instalá-lo. É preciso estar atento a essas permissões, pois elas indicam possíveis vetores de ataque que serão postos em prática pelo aplicativo.

Sistema de reputação: Um modo de se obter informações de um software é através do sistema de reputação existente na maioria das lojas de aplicativos. A partir dos comentários e notas dados por usuários que já instalaram o referido aplicativo, é possível ter uma noção da confiabilidade do mesmo.

Atualização da plataforma: Sempre que possível, mantenha o dispositivo atualizado com a versão mais recente disponível do sistema operacional, pois as vulnerabilidades encontradas só serão resolvidas através dessas atualizações.

3.3 BEST SECURITY PRACTICES FOR ANDROID, BLACKBERRY AND IOS (OH *ET AL.*, 2012)

Essa referência foi utilizada como uma das principais do trabalho pelo fato de possuir objetivo semelhante ao da cartilha desenvolvida. No documento são listadas algumas boas práticas, e algumas dessas serviram de inspiração para parte do conteúdo proposto na cartilha. Os registros a seguir são resultados da análise do documento.

Junto com o aumento do uso do *smartphones*, os dados confidenciais e pessoais armazenados em plataformas móveis têm aumentado. Além disso, *malwares* (*softwares* maliciosos) disponíveis para esses dispositivos aumentaram a um ritmo alarmante.

A lista das melhores práticas de segurança nesse documento foi compilada pelo *ranking* de práticas que atenuem ou tentam impedir o acesso não autorizado e a perda da confidencialidade.

A prevenção de ataques de softwares maliciosos pode ser a melhor maneira para o usuário garantir a segurança em seu dispositivo. Segundo (OH *et al.*, 2012) devem ser tomadas as seguintes decisões:

Definir uma senha para o dispositivo: Essa prática age como primeira linha de defesa contra qualquer acesso físico não autorizado ao dispositivo. Existem diversas maneiras de se bloquear a tela do Android, como foi mostrado anteriormente neste trabalho (padrão de desenho, PIN ou senha).

Desativar a instalação de aplicativos a partir de fontes desconhecidas: Por se tratar de uma plataforma aberta, qualquer fornecedor pode desenvolver um aplicativo para a plataforma Android. Aplicações disponíveis fora da *Google Play* estão em um alto risco de conter programas potencialmente perigosos, que podem causar sérias ameaças.

Instalar proteção anti-vírus: Aplicativos anti-vírus evitam que aplicações maliciosas sejam instaladas e detectam aplicações maliciosas já instaladas. Recomenda-se a instalação de um aplicativo a partir da *Google Play*, com base na classificação dos usuários, avaliações e revisão.

Avaliar permissões de aplicações: Aplicativos instalados exigem permissões para realização de atividades. As permissões podem acessar partes do dispositivo que a sua funcionalidade não justifica. Recomenda-se ler com atenção e compreender as

permissões a serem concedidas, antes de instalar qualquer aplicativo, para que aplicativos maliciosos sejam evitados.

Verificar atualizações do sistema: As atualizações do *software* podem incluir programas para corrigir falhas de segurança presentes no dispositivo.

Desligar recursos de conexão sem fio (GPS, *Bluetooth, Wi-Fi e Hotspot)* quando não estiverem sendo utilizados: O ato de se conectar a redes e/ou dispositivos desconhecidos pode levar a sérias ameaças. Por exemplo, o compartilhamento de conexão com outros dispositivos pode resultar em perda de dados durante o tráfego.

Não ative o modo *Root*: Alguns recursos que poderiam ser utilizados para melhorar o sistema Android foram desabilitados de fábrica. O processo de *root* cede ao usuário o acesso total ao dispositivo, podendo deixar o sistema aberto a vulnerabilidades.

Consciência de segurança na WEB: Transações sensíveis, como aplicações bancárias, têm grandes chances de serem interceptadas. Deve-se apenas fazer essas transações em redes sem fios de confiança, ou a partir de conexão do próprio celular.

Fazer *backup* dos dados: Fazer *backup* dos dados permite aos usuários que restaurem automaticamente seus dados a partir do *backup* em nuvem.

Desativar localização da Google: Serviços de localização da Google fornece aplicativos com a localização do dispositivo sem o uso de GPS. Aplicações nocivas podem utilizar dados de localização para encontrar usuários.

3.4 ANALISE COMPARATIVA COM CARTILHAS EXISTENTES

Como referencial teórico pode-se citar também duas cartilhas de segurança para dispositivos móveis já existentes. Tratam-se respectivamente da cartilha desenvolvida pelo CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) (CERT.BR., 2012) e da cartilha desenvolvida pelo CAIS/RNP (centro de atendimento e incidentes da Rede Nacional de Ensino e Pesquisa) (CAIS/RNP, 2012). Ambas foram publicadas no ano de 2012.

Do mesmo modo que a cartilha proposta visa sugestões para mitigar riscos de segurança no uso de dispositivos móveis, as cartilhas já existentes possuem o mesmo intuito. Porém, pelo fato de as mesmas terem sido publicadas no ano de 2012, este trabalho caracterizou-se pela busca de novas sugestões para auxiliar aos usuários ao

tomar decisões de configuração do seu dispositivo. No documento proposto pelo trabalho foi adicionada a sugestão de ~~ao~~ ativar o modo roteador de Wi-Fi (*hotspot)*. É necessário que haja preocupação com a existência e manutenção de uma senha, para que o acesso se torne restrito apenas a dispositivos que tenham conhecimento da mesma. Os principais fundamentos para a escrita da cartilha foram identificados após leitura de artigos, e inclusive, do relatório da Google referente à segurança em dispositivos móveis com o sistema operacional Android durante o ano de 2014.

A cartilha resultante deste trabalho diferencia-se das cartilhas já escritas pelo fato de estar direcionada para dispositivos com o sistema operacional Android, e por ser uma cartilha que possui uma aplicação, também desenvolvida durante este trabalho, como solução integrada a fim de garantir que tomadas de decisões sugeridas estão sendo de fato seguidas.

4 ESTRATÉGIA PARA A MELHORIA DE SEGURANÇA DE DISPOSITIVOS MÓVEIS BASEADOS EM ANDROID

Nos capítulos anteriores foram relatados o expressivo aumento do número de dispositivos móveis e a maior utilização desses dispositivos para atividades que antes eram utilizadas apenas por computadores, o que acarreta, dentre outras coisas, em uma maior quantidade de dados trafegados nesses dispositivos móveis. Foi ainda citada a considerável taxa de aceitação do sistema operacional Android e a atração de usuários maliciosos a desenvolverem aplicações que infringem a segurança dos dispositivos nos quais são instalados.

Diante desses fatores, tornou-se mais comum a ocorrência de ataques a dispositivos móveis com o sistema operacional Android, com a finalidade de interceptar os dados trafegados. Para tal, foi elaborada uma estratégia composta por uma cartilha autoexplicativa e por uma aplicação que provê suporte tecnológico a esta cartilha.

4.1 CARTILHA DE SEGURANÇA PARA DISPOSITIVOS MÓVEIS

As subseções anteriores reiteram a existência de riscos de segurança provenientes da má gestão/configuração dos dispositivos a partir do usuário, como também, adoção de práticas indevidas.

Devido a esses fatores, tornou-se importante a necessidade da criação de uma cartilha composta por sugestões que devem ser tomadas pelo usuário final (especialmente o usuário não-técnico, que não tem familiaridade com conceitos de computação e segurança) com a finalidade da mitigação desses riscos de segurança. Essas sugestão são apresentadas e explicadas nas próximas subseções.

4.1.1 Evitar Dispositivos que Tenham Sido Ilegalmente Desbloqueados

Denomina-se como *root* o desbloqueio do sistema operacional de um dispositivo móvel. Uma vez que esse modo é ativo, o dispositivo passa a não respeitar a conduta de segurança prescrita pela Google. Os aparelhos já vêm de fábrica com o modo *root* inativo. Sugere-se que o usuário não ative esta função, pois, uma vez ativa, o usuário passará ter permissão para a realização de qualquer atividade, tornando-o mais vulnerável a ataques de segurança, pelo fato de o modo *root* possibilitar ao usuário o perfil de superusuário. Esse usuário pode realizar atividades que antes só eram possíveis com o perfil de administrador. Uma dessas atividades é inserir no dispositivo versões

personalizadas do Android, que por muitas vezes vêm de fontes terceiras e desconhecidas. Nessas versões personalizadas podem estar contidos *softwares* maliciosos com a intenção de acessar ou tomar posse dos dados do usuário.

4.1.2 Manter a Versão do Android e a Versão dos Aplicativos Sempre Atualizadas

Quando uma nova ameaça é descoberta, o Android disponibiliza *patches (*programas de computador criado para atualizar ou corrigir um *software)* de segurança. Existe a opção de deixar que o dispositivo e as aplicações sejam atualizados automaticamente. Pois, para aplicativos, também há a atualização de sua versão com a finalidade da correção de erros descobertos após seu lançamento para os usuários. A sugestão é que essa opção seja ativa, ou que seja função do usuário verificar frequentemente versões atualizadas tanto para seu sistema operacional, ou como para seus aplicativos. Por exemplo, no ano de 2014 o Android desenvolveu 79 *patches* de segurança (GOOGLE, 2014).

4.1.3 Ser Cuidadoso ao Instalar Aplicações Através de Sites Externos à Loja Oficial do Android

Aplicativos enviados à Google Play são analisados e classificados quanto à segurança. Essa análise é feita pela própria Google, a partir de um sistema chamado *Bouncer*. *O Bouncer* é um que sistema verifica o APP e detecta comportamentos possivelmente suspeitos. Portanto, o risco de se instalar um aplicativo nocivo dentro da loja oficial é inferior ao risco de aplicações instaladas a partir de sites terceiros, pois, a instalação de aplicativos a partir de lojas externas não é verificada pelo sistema *Bouncer*. Consequentemente, a aplicação não será avaliada e não se terá conhecimento de seus possíveis riscos.

4.1.4 Manter Interfaces de Comunicação como *Bluetooth, Wi-fi* e Redes Móveis Habilitadas Apenas Quando Necessário

Por conter uma grande quantidade de informações pessoais armazenadas no dispositivo, a interceptação de dados no tráfego é bastante atrativo aos invasores. Sugere-se então que se deixe apenas ativas as interfaces que estejam em uso. É possível ter acesso a dados do dispositivo através de conexão via redes sem fio. Em condições normais, essa comunicação entre dispositivos se dá apenas com autorização dos dispositivos envolvidos. Porém, com a finalidade de acesso a dados pessoais sem que

haja autorização do proprietário, é possível a intercepção de dados a partir da execução de *softwares* maliciosos que são capazes de prover a conexão entre dispositivos sem que o proprietário do dispositivo "vítima" seja notificado.

4.1.5 Não Seguir Links Recebidos por Meio de Mensagens Eletrônicas

Sugere-se que evite clicar em *links* recebidos através de mensagens eletrônicas pois, é comum a utilização de *links* para ações com fins maliciosos. Há a possibilidade de, ao clicar em *links* desconhecidos, o usuário fornecer, sem querer, informações confidenciais.

Mesmo que tenha sido enviada por pessoas conhecidas/de confiança, o ideal é que se confirme antes de abrir o *link.* Pois, muitas vezes nem o próprio remetente sabe do envio, uma vez que anteriormente já foi vítima do ataque, o que o faz repassar o conteúdo automaticamente para os seus contatos.

4.1.6 Inserir um Bloqueio de Tela

Logo que uma terceira pessoa entra em contato físico com um dispositivo, o primeiro contato é com a tela de bloqueio. Quanto mais protegida estiver a tela, menor é a probabilidade de o agente ter acesso às informações contidas no dispositivo móvel.

O Android permite ao usuário cinco modos de bloqueio de dela: Reconhecimento facial, padrão de desenho, PIN, senha e reconhecimento de impressão digital. Recomenda-se que o proprietário faça de um desses modos oferecidos pelo sistema operacional o seu controle de acesso padrão.

Os meios mais seguros são o reconhecimento de impressão digital ou a senha. O reconhecimento facial pode ser facilmente forjado ao posicionar uma foto do proprietário no sensor da câmera do dispositivo. Já o desenho padrão pode ser facilmente descoberto por um algoritmo, uma vez que é basicamente uma matriz de ordem 3X3, ou ainda pela mancha que os dedos deixam na tela, pois, o usuário repete o desenho sempre que deseja usar o seu aparelho.

4.1.7 Antes de Instalar uma Aplicação, Ler as Permissões que a Mesma Requisita Ter Acesso

Todos os aplicativos ao serem instalados em um dispositivo com a plataforma Android possuem uma lista de permissões. É essencial que o usuário leia e tenha ciência

do que está permitindo para cada aplicação, com a finalidade de evitar instalações que requerem permissões que fogem do objetivo da aplicação.

É de grande importância que o usuário leia essas informações para ter conhecimento de quais informações cada aplicativo terá acesso. Algumas aplicações têm funcionalidades que requerem mais permissões do que as necessárias para a execução de suas atividades. Quando isso ocorre, pode se tratar de um aplicativo malicioso, pois, quando o acesso é permitido, o aplicativo tem total acesso às informações, podendo o agente utilizar desses dados para fins quaisquer.

4.1.8 Remover Os Dados Do Dispositivo Em Caso De Perda/Roubo

A ameaça de maior probabilidade de ocorrência é o extravio do dispositivo, principalmente quando são inseridas aplicações maliciosas. Portanto, em caso de perda ou roubo de seu dispositivo, selecione a limpeza remota, que é responsável por apagar todos os dados do aparelho e redefinir a configuração original. Para que a limpeza remota seja realizada, é preciso que o usuário tenha em seu dispositivo uma conta da Google vinculada, através da autenticação de seu *e-mail* e senha.

Para fazer a limpeza remota é necessário que sejam seguidos esses passos:

1) Em qualquer navegador da WEB, acessar admin.google.com
2) Fazer *login* no Google *Admin Console*
3) Selecionar em Gerenciamento de dispositivos a opção Dispositivos móveis;
4) Selecionar o dispositivo que se deseja limpar;
5) Optar por Limpeza Remota ou Limpar Conta;
6) Uma segunda caixa aparece solicitando a confirmação da limpeza remota.

Geralmente, o dispositivo recebe o comando de limpeza remota dentro de alguns segundos. Entretanto, às vezes o comando não chega ao dispositivo imediatamente. O aplicativo Google *Apps Device Policy* verifica o servidor a cada três horas para identificar se há um comando de limpeza. Portanto, o tempo máximo até que o dispositivo seja limpo é de cerca de três horas ou até que o dispositivo seja reconectado à rede.

4.1.9 Ativar o serviço de Verificação de Aplicativos

Pelo fato de o Android ser uma plataforma que permite a instalação de aplicativos originados de lojas externas à loja oficial, a Google analisou a necessidade de existir maior controle dos dispositivos e seus aplicativos. Conforme já citado anteriormente, para aplicativos da loja oficial, a Google Play, foi adicionada a varredura a partir do *Bouncer*. Portanto, a Google desenvolveu um sistema chamado Verify Apps com o intuito de realizar a varredura nos dispositivos para buscar por vulnerabilidades em aplicativos externos a sua loja oficial. Na semana anterior a 1º de novembro de 2014, o *Verify Apps* escaneou mais de 200 milhões de dispositivos apenas em um dia (GOOGLE, 2014). Sugere-se, no entanto, a ativação do serviço de verificação de aplicativos para que seja realizada a busca de aplicativos com comportamento possivelmente malicioso.

4.1.10 Não Permitir a Instalação de Aplicativos a Partir de Fontes Desconhecidas

Para que haja um maior controle de quais aplicativos estão sendo instalados, os dispositivos com o sistema operacional Android vêm configurado de modo a não permitir instalações originadas de fontes desconhecidas. Porém, basta o usuário acessar o menu de configurações, que terá acesso a habilitar a permissão da instalação. Essa prática não é recomendada pelo fato de nas lojas oficiais haver a verificação dos aplicativos com a finalidade de buscar por comportamentos maliciosos, no momento em que os mesmos são enviados à loja. Diferente das aplicações de fontes externas, que só serão analisadas após a instalação, caso o *Verify Apps* esteja ativo.

4.1.11 Ao ativar o roteador de *WiFi (hotspot)* manter uma senha para controle de acesso à rede.

É possível tornar um dispositivo móvel em um roteador *WiFi.* Ao acessar o menu de configurações do dispositivo, há a funcionalidade que permite que o usuário compartilhe sua rede e permita que outros dispositivos tenham acesso à internet, por exemplo, a partir de seu aparelho. O risco ao tornar ativa essa funcionalidade se dá em casos em que o acesso à rede roteada não utiliza um controle de acesso através do uso de senha. Pois, pessoas má intencionadas podem entrar nessa rede e interceptar dados sem que o proprietário da informação tenha conhecimento do ocorrido. Atualmente, o sistema Android já fornece ao usuário uma senha quando o mesmo ativa o modo roteador em seu dispositivo. Sugere-se que essa senha seja mantida, e caso haja a

desconfiança de que outros dispositivos desconhecidos estão tendo acesso à rede, sugere-se que a mesma seja trocada.

4.2 APLICAÇÃO

Em conjunto à cartilha desenvolvida, que contempla boas práticas sugeridas para o usuário com a finalidade de se obter um uso mais cauteloso do dispositivo móvel em relação aos ataques de segurança, foi implementada uma aplicação *mobile* específica para a plataforma Android. Mesmo estando em sua versão inicial, essa aplicação tem como objetivo principal verificar a execução de itens encontrados na cartilha proposta.

A Figura 2 representa a tela inicial da aplicação. Ao clicar no botão “Procurar Vulnerabilidades”, o usuário permite que aplicação verifique a existência de comportamentos que possam deixar em risco os dispositivos e as informações nele contidas.

Figura 2. Tela inicial da aplicação desenvolvida.

Fonte: Elaborada pela autora.

A aplicação foi desenvolvida sobre a plataforma de desenvolvimento Eclipse, em conjunto com o Android SDK, ferramenta que oferece aos desenvolvedores de software móvel a chance de desenvolver aplicações para Android, e da linguagem de programação JAVA (GOOGLE, 2015).

Para implementar a funcionalidade da aplicação, “Procurar Vulnerabilidades”, são utilizadas funções disponibilizadas na *API* (*Application Programming Interface* ou, em português, Interface de Programação de Aplicativos.) pela própria Google e aberta a todos assim como o código fonte do Android, por se tratar de um *software* de código aberto.

A Figura 3 representa o trecho de código referente a quatro das verificações presentes até então na aplicação. Uma vez que o usuário clica para buscar pelas vulnerabilidades, opção na tela principal da aplicação, cabe ao aplicativo verificar se o dispositivo está com *wi-fi, bluetooth* ou GPS ativos. É funcionalidade também do aplicativo verificar se o dispositivo possui algum bloqueio de tela como controle de acesso, e se possui em seu dispositivo a versão do Android mais recente, instalada. Caso não possua, o usuário recebe um aviso de que seu dispositivo está sem um modo de tela ativo.

Figura 3. Trecho do código referente à busca de vulnerabilidades.

```
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.activity_main);
    verificaTudo=(Button)findViewById(R.id.verifyAll);
    verificaTudo.setOnClickListener(new View.OnClickListener() {
        public void onClick(View v) {
            WifiManager wifi = (WifiManager) getSystemService(Context.WIFI_SERVICE);
            // Verifica se a Wi-Fi está ativa, e retorna essa mensagem ao usuário caso seja verdadeiro.
            if (wifi.isWifiEnabled()) {
                Toast.makeText(MainActivity.this,
                        R.string.conectado,Toast.LENGTH_SHORT).show();
            }

            BluetoothAdapter mBluetoothAdapter = BluetoothAdapter.getDefaultAdapter();

            // Verifica se o bluetooth está ativo, e retorna essa mensagem ao usuário caso seja verdadeiro.
            if (mBluetoothAdapter.isEnabled()) {
                Toast.makeText(MainActivity.this,
                        R.string.bluetooth_conectado,Toast.LENGTH_SHORT).show();
            }

            // Verifica se o GPS está ativo, e retorna essa mensagem ao usuário
            LocationManager gps = (LocationManager) getSystemService(Context.LOCATION_SERVICE);
            if (gps.isProviderEnabled(LocationManager.GPS_PROVIDER)) {
                Toast.makeText(MainActivity.this,
                        R.string.gps_conectado,Toast.LENGTH_SHORT).show();
            }
            // Verifica se o dispositivo possui ao menos um modo de bloqueio de tela ativo
            if (isDeviceInsecured()){
                Toast.makeText(MainActivity.this,
                        R.string.sem_bloqueio,Toast.LENGTH_SHORT).show();
            };
        }
    });
}
```

Fonte: Elaborado pela autora.

O código presente na Figura 4 é responsável por verificar se o dispositivo possui como modo de bloqueio de tela um dos modos mais seguros, que são a senha e o reconhecimento de digitais. Essa função é utilizada na chamada principal da aplicação para que, uma vez que o usuário inicialize a aplicação, ela esteja apta a dar ao mesmo um retorno de que o seu aparelho possui ou não um meio de controle de acesso.

Figura 4. Trecho do código referente à verificação do modo de controle de acesso no dispositivo móvel.

```
private boolean isDeviceInsecured() {
    String LOCKSCREEN_UTILS = "com.android.internal.widget.LockPatternUtils";
    try {
        Class<?> lockUtilsClass = Class.forName(LOCKSCREEN_UTILS);
        Object lockUtils = lockUtilsClass.getConstructor(Context.class).newInstance(this);
        Method method = lockUtilsClass.getMethod("getActivePasswordQuality");
        int lockProtectionLevel = (Integer)method.invoke(lockUtils);
        if(lockProtectionLevel >= DevicePolicyManager.PASSWORD_QUALITY_NUMERIC)
        {
            return false;
        }
    }
    catch (Exception e) {
        Log.e("reflectInternalUtils", "ex:"+e);
    }
    return true;
}
```

Fonte: (STACKOVERFLOW, 2013).

Na sua versão atual, esta aplicação contempla um subconjunto das funções básicas dos itens existentes na cartilha. Ficando, portanto, como trabalho futuro a implementação das funcionalidades restantes.

A aplicação contempla cinco principais funcionalidades. São elas:

1) **Verificar o status da *wi-fi:*** A aplicação retorna ao usuário se a *wi-fi* está ativa;
2) **Verificar status do *bluetooth:*** A aplicação retorna ao usuário se o *bluetooth* está ativo;
3) **Verificar o status do *GPS:*** A aplicação retorna ao usuário se o GPS está ativo;
4) **Verificar se o dispositivo possui bloqueio de tela para controle de acesso:** A aplicação retorna ao usuário a informação de que o dispositivo não possui um dos modelos de bloqueio de tela mais seguros, caso o mesmo não possua configurado um dos modos como bloqueio de tela.
5) **Verificar se a versão do Android no dispositivo corresponde à versão atual mais recente disponibilizada pelo Google:** A aplicação

retorna ao usuário a informação de que o dispositivo está com a versão desatualizada caso a versão do Android instalada no mesmo seja inferior à versão mais recente disponibilizada pela Google.

A Figura 5 ilustra uma situação hipotética onde o usuário não ativou um bloqueio de tela em seu dispositivo. Ao clicar em “Procurar Vulnerabilidades”, o aplicativo identificou a ausência de um controle de acesso do tipo bloqueio de tela mais seguro, e retornou essa mensagem ao usuário.

Figura 5. Captura de tela simulando um dispositivo sem bloqueio de tela seguro.

Fonte: Elaborada pela autora.

4.3 MODELAGEM DA APLICAÇÃO

Nesta seção será apresentada a modelagem utilizada para o desenvolvimento do aplicativo.

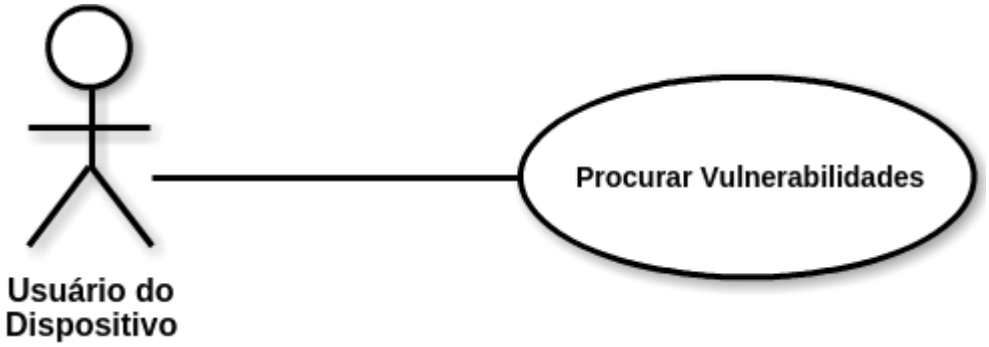
Para a construção do aplicativo foi realizada a implementação de cinco funcionalidades com o objetivo de verificar se algumas das práticas sugeridas na cartilha estão sendo seguidas. Essas cinco funcionalidades são verificadas logo após a

realização do clique no botão Procurar Vulnerabilidades, presente na tela principal da aplicação.

O sistema contém como ator o usuário do aplicativo, e como caso de uso a procura de vulnerabilidades.

Optou-se por modelar o *software* a partir da apresentação do diagrama de caso de uso representado pela Figura 6, pela identificação desse caso de uso e pela representação do modelo de negócios do caso de uso, através da representação a partir do modelo BPMN (*Business Process Modeling Notation*), padrão para a criação de modelos de processo.

Figura 6. Diagrama de caso de uso do aplicativo desenvolvido.



Fonte: Elaborada pela autora.

A Figura 6 representa o diagrama de caso de uso procurar vulnerabilidades. O ator, usuário do dispositivo, possui como representação gráfica a imagem utilizada, e a função a ser realizada (o caso de uso) é representado pelo balão.

4.3.1 IDENTIFICAÇÃO DO CASO DE USO

Nome

Caso de Uso 01 – Procurar Vulnerabilidades

Descrição

Este caso de uso tem o objetivo de verificar buscar por vulnerabilidades no dispositivo Android.

Atores Envolvidos

Dono do Dispositivo

Pré-condição

O aplicativo precisa estar instalado no dispositivo e o botão “Procurar Vulnerabilidades” ter sido clicado

Pós-condição

Após o fim do caso de uso, o usuário deve estar ciente de quais vulnerabilidades estão presentes no dispositivo.

Fluxo de Eventos Principal

1. O usuário clica no botão “Procurar Vulnerabilidade”.
2. O aplicativo verifica se a rede *wi-fi* está ativa.
3. O sistema devolve uma mensagem sugerindo ao usuário a inativação da rede caso ela esteja sem uso.
4. O aplicativo verifica se o *Bluetooth* está ativo.
5. O sistema devolve uma mensagem sugerindo ao usuário a inativação da conexão sem fio via *bluetooth* caso ela esteja sem uso.
6. O aplicativo verifica se a localização por GPS está ativa.
7. O sistema devolve uma mensagem sugerindo ao usuário a inativação do compartilhamento de localização pelo uso do GPS caso ela esteja sem uso.
8. O aplicativo verifica se algum dos modelos de bloqueio de tela mais seguros está ativo.
9. O sistema devolve uma mensagem para o usuário informando que o dispositivo não possui um dos modelos mais seguros de bloqueio de tela.
10. O aplicativo verifica se a versão atual do Android instalada é inferior à mais recente desenvolvida e disponível.
11. O sistema devolve uma mensagem para o usuário, informando que a versão instalada em seu dispositivo não é a mais recente, e recomenda que o usuário busque por informações da versão mais atual disponibilizada para seu dispositivo.
12. O aplicativo verifica se o modo *root* está ativo no dispositivo.
13. O sistema devolve ao usuário a informação de que o modo *root* está ativo, e sugere a desativação do mesmo.
14. O aplicativo verifica se a instalação de aplicações oriundas de fontes desconhecidas está ativa.
15. O sistema devolve uma mensagem para o usuário informando que aplicações originadas de fontes desconhecidas podem ser instaladas em seu dispositivo. Será também sugerido que esta configuração seja desabilitada.
16. O aplicativo verifica se no dispositivo está ativa a função de verificar aplicações.
17. O sistema devolve uma mensagem para o usuário informando que a verificação das aplicações não está sendo realizada, e sugere a ativação da mesma.

18. O caso de uso é finalizado.

Fluxo Secundário ou Alternativo [FS001]: Levando em consideração que no passo 2 o sistema retornou que a *Wi-Fi* está desligada, o passo 3 não é realizado pois nenhuma mensagem é retornada para o usuário.

Fluxo Secundário ou Alternativo [FS002]: No caso de o passo 4 verificar que o *bluetooth* está inativo, o passo 5 não é realizado e nenhuma mensagem é retornada para o usuário.

Fluxo Secundário ou Alternativo [FS003]: Ao considerar que no passo 6 o compartilhamento da localização via GPS está inativo, nenhuma mensagem é retornada para o usuário e o passo 7 não é realizado.

Fluxo Secundário ou Alternativo [FS004]: Sendo verificado no passo 8 que o dispositivo já possui como bloqueio de tela uma das formas mais seguras, o passo 9 não é realizado por não ser necessário o retorno de mensagens de aviso para o usuário.

Fluxo Secundário ou Alternativo [FS005]: Ao ser registrado no passo 10 que a versão do Android instalada no aplicativo é mais recente, nenhuma mensagem é retornada ao usuário. Consequentemente, não é necessária a realização do passo 11.

Fluxo Secundário ou Alternativo [FS006]: Ao ser realizado o passo 12 e analisado que no dispositivo não está ativo o modo *root*, nenhuma mensagem é retornada para o usuário e o passo 13 não é realizado.

Fluxo Secundário ou Alternativo [FS007]: Após realizado o passo 14 e constatado que a instalação a partir de fontes desconhecida não está sendo permitida, não se retorna mensagem ao usuário e o passo 15 não é necessário.

Fluxo Secundário ou Alternativo [FS008]: Ao realizar o passo 16 e concluir que a verificação de aplicações está sendo realizada, o aplicativo não retorna mensagem para o usuário do dispositivo e o passo 17 não é realizado.

Para a versão atual da aplicação foram desenvolvidos alguns dos passos descritos no caso de uso. As funcionalidades implementadas correspondem ao comportamento da aplicação a partir do passo 1 e têm finalização no passo 11. Portanto, para a modelagem do modelo de negócio tem-se que a finalização do caso de uso se dá no passo 12. A continuação da implementação da aplicação se encontra como planos para trabalhos futuros.

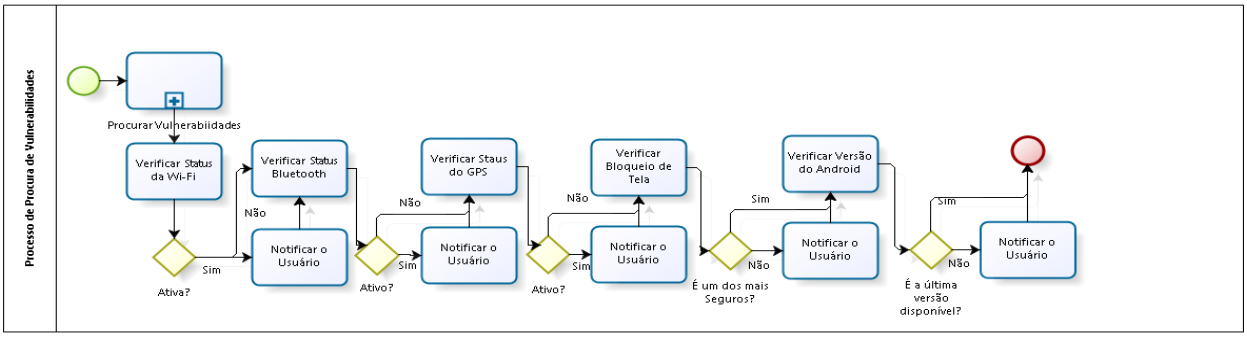
Optou-se por também modelar o *software* a partir do modelo de negócios para facilitar o entendimento de todos os processos a serem realizados, como também, o

comportamento dos mesmos, pois esses variam de acordo com o retorno da chamada da função no aplicativo.

A figura 7 representa o modelo de negócios do aplicativo a partir do modelo BPMN. Para a construção da mesma foi utilizada a ferramenta Bizagi (BIZAGI, 2015). Trata-se de um *software desktop* gratuito para a construção de modelos de processo.

Para a representação da aplicação, adotou-se a atividade de Procurar Vulnerabilidades como um processo, e para tal, foram criados cinco sub processos com comportamentos a serem determinados após verificação de condicional. Porém, independente da resposta da condição do sub processo anterior, todos os processos serão efetuados. A importância de verificar o condicional se dá no que se refere a devolver informações para o usuário.

Figura 7 Modelo de negócios do processo de procurar por vulnerabilidades.



Fonte: Elaborado pela autora.

5 AVALIAÇÃO

Foram utilizados dois métodos para avaliação. Realizou-se entrevistas para coletar dados referentes ao comportamento do usuário comum em relação ao uso de seu dispositivo, com o intuito de listar os mais reincidentes riscos aos quais os aparelhos estavam vulneráveis e listá-los na cartilha. Testou-se também a aplicação para verificar sua relevância, tendo em consideração que seu objetivo é auxiliar o usuário a seguir as boas práticas sugeridas na cartilha.

Com a finalidade de observar pontos importantes para serem definidos como boas práticas defendidas pela cartilha, optou-se pela realização uma entrevista na qual, os usuários entrevistados afirmavam se era de seu conhecimento o risco causado ao não tomar algumas das decisões propostas. Deu-se a preferência aos usuários comuns, aqueles que não possuem grandes informações sobre computação e segurança da informação. Perguntou-se, por exemplo, se o usuário atualmente já possui em seu dispositivo móvel algum controle de acesso. Possuir um controle de acesso nos dispositivos móveis é uma das dez sugestões de boas práticas encontradas na cartilha.

Adicionalmente, a fim de avaliar os itens sugeridos na cartilha e de validar a proposta composta pela mesma em conjunto com o aplicativo, foram realizados testes em dispositivos Android para verificar a ocorrência/ausência das boas práticas encontradas solução integrada. Optou-se por fazer os testes em dispositivos cujos usuários não têm grande acesso à segurança da informação, seus riscos e causas. Verificou-se em 15 dispositivos o comportamento da aplicação.

5.1 ANÁLISE DA ENTREVISTA

A entrevista é uma das técnicas mais utilizadas, atualmente, em trabalhos científicos. Ela permite ao pesquisador extrair uma quantidade muito grande de dados e informações que possibilitam um trabalho bastante rico (BRITO JÚNIOR; FERES JÚNIOR, 2011). Optou-se pela entrevista pelo fato de haver uma comunicação mais direta, devido a interação do entrevistador com o entrevistado, diferente do que ocorre em um questionário. Os questionários não são adequados para obter opiniões aprofundadas, identificar problemas ou soluções para um sistema (OLIVEIRA, 2000).

Portanto, além se tratar da avaliação dos itens a serem inseridos na cartilha, a entrevista foi realizada com o intuito de ouvir o usuário na tentativa de obter novas

informações com a possibilidade de adicioná-las à cartilha como sugestão de boa prática, para amenizar a exposição dos dispositivos móveis a ataques de segurança por parte dos entrevistados.

5.1.1 DADOS DA ENTREVISTA

- Início: 09/07/2015
- Término: 13/07/2015

Observação: Como pré-condição da entrevista, fez-se necessária a apresentação do assunto a ser abordado. Para tal, leu-se o resumo do projeto.

1) Olá, gostaria de saber um pouco sobre você. Qual seu nome e sua idade? Afirmo que esses dados serão confidenciais, e servirão apenas para cálculos estatísticos.
2) Você se preocupa com a segurança da informação em seu dispositivo móvel? Em caso afirmativo, o que você faz para garantir essa segurança?
3) Você mantém a versão do seu Android atualizada?
4) Você mantém interfaces de comunicação como *bluetooth*, *wi-fi*, GPS e redes móveis ativas apenas quando necessário?
5) Você clica em *links* recebidos por meio de mensagens eletrônicas ou SMS?
6) Seu dispositivo possui bloqueio de tela? Em caso afirmativo, você poderia nos informar qual modo de controle de acesso você utiliza?
7) Você lê as informações referentes às permissões dos aplicativos antes de instalá-los?
8) Você sabia que em caso de perda ou roubo é possível remover os dados de seu dispositivo através da ferramenta *Admin* Console, que pode ser aberta em qualquer navegador?
9) Você gostaria de ter acesso a uma cartilha com sugestões de boas práticas para reduzir o risco a ataques de segurança em seu dispositivo móvel?
10) Você gostaria de/utilizaria uma aplicação para garantir que sugestões contempladas na cartilha estão sendo seguidas?

Muito obrigado pela sua atenção.

Thaís Antunes Bione.

Para a obtenção dos resultados foram escolhidas 15 pessoas com idade entre 19 e 59 anos. Tentou-se verificar se havia alguma diferença de comportamento do usuário em função da idade, o que não se concluiu, pois, houve casos em que pessoas com maior idade responderam às perguntas do questionário tendendo a um perfil que corresponde ao uso menos vulnerável a riscos de segurança, que outras mais jovens, os quais *a priori* poderiam ter um comportamento mais arriscado. O que também não afirma que os mais jovens possuem o uso mais vulnerável. A definição dos tipos de usuário como, por exemplo, o usuário com maior probabilidade a ataques de segurança, é obtida através do nível de informação que o mesmo tem sobre computação e segurança da informação, e não a idade que possuem.

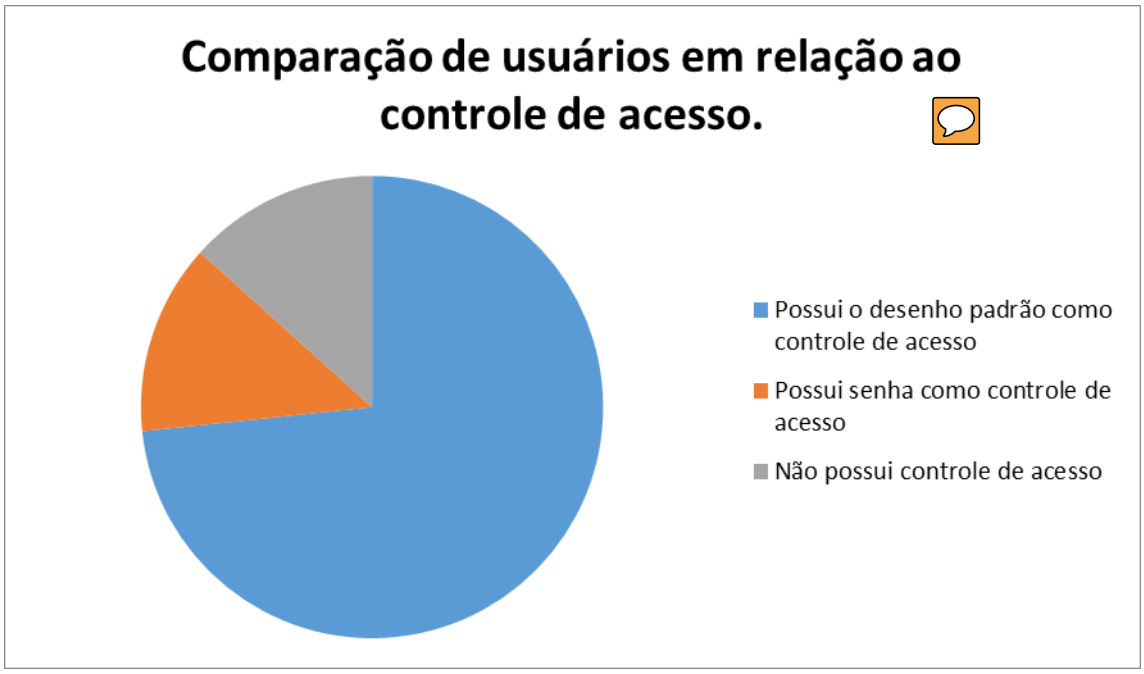
Fez parte também da entrevista o questionamento sobre se o usuário se preocupa com a segurança de seu dispositivo. Aproximadamente 67% afirmaram se preocupar, mas apenas 20% afirmaram que leem as permissões que os aplicativos requerem acesso ao serem instalados. Ou seja, 80% dos entrevistados não leem as permissões, o que pode levá-los a sérios problemas no que diz respeito à segurança de suas informações. Isso ocorre uma vez que o aplicativo consegue ter acesso às informações do usuário, já que ficam sob posse do agente (aplicativo). Cabe ao agente optar ou não por utilizar essas informações para fins maliciosos, como a extorsão de dinheiro para que haja a devolução dos dados, por exemplo.

Dos 15 entrevistados, aproximadamente 67% afirmaram se preocupar com a segurança da informação, mas não sabem como garanti-la. Os restantes 33% afirmaram não se preocupar com a segurança da informação.

Ainda em relação aos usuários que afirmam se preocupar com a segurança da informação de seus dispositivos, 74% afirmam que possuem bloqueio de tela para controle de acesso com o modelo de desenho padrão, ou seja, modelo baseado numa matriz 3X3, facilmente quebrado por algoritmos (TEDESCHI, 2010). 13% afirmam que não tem controle de acesso em seu dispositivo, e apenas os 13% restantes afirmam que possuem como modo de controle de acesso a inserção de uma senha numérica. Nenhum dos três modos é classificado como as duas mais seguras, que são o reconhecimento de digital ou a senha alfanumérica.

A Figura 8 ilustra graficamente a opção dos usuários entrevistados por um dos modos de controle mais frágeis, o modo padrão. 74% dos usuários utilizam esse modo de bloqueio de tela para controle de acesso em seu dispositivo.

Figura 8. Comparação de usuários em relação ao controle de acesso.



Fonte: Elaborada pela autora.

Dentre as perguntas feitas durante as entrevistas, fez-se presente o questionamento referente à atualização das aplicações e do sistema operacional Android. Como resultado, foi obtido que 13% informaram não saber sobre as atualizações por não se preocuparem, 67% afirmaram manter atualizado, pois, receberam uma notificação automática e 20% afirmaram não atualizar para que o espaço da memória de seu dispositivo não seja reduzido.

Ao término da entrevista ficou claro que embora 67% dos usuários tenham a preocupação com a segurança de seus dispositivos, uma boa parte realiza algumas ações que deixam seus dispositivos mais vulneráveis a ataques.

Ainda se fizeram presentes na entrevista questionamentos sobre se o usuário teria interesse em visualizar a cartilha, e de instalar a aplicação que o auxiliasse verificando se as boas práticas sugeridas estão de fato sendo seguidas. As respostas foram positivas para todos os usuários nos dois casos, 100% dos entrevistados afirmaram ter interesse pela cartilha e pela instalação da aplicação.

5.2 RESULTADOS DA AVALIAÇÃO DA APLICAÇÃO DESENVOLVIDA

Com o intuito de auxiliar o usuário a seguir as sugestões encontradas na cartilha, foi desenvolvido um aplicativo. Testou-se a aplicação em aparelhos de usuários

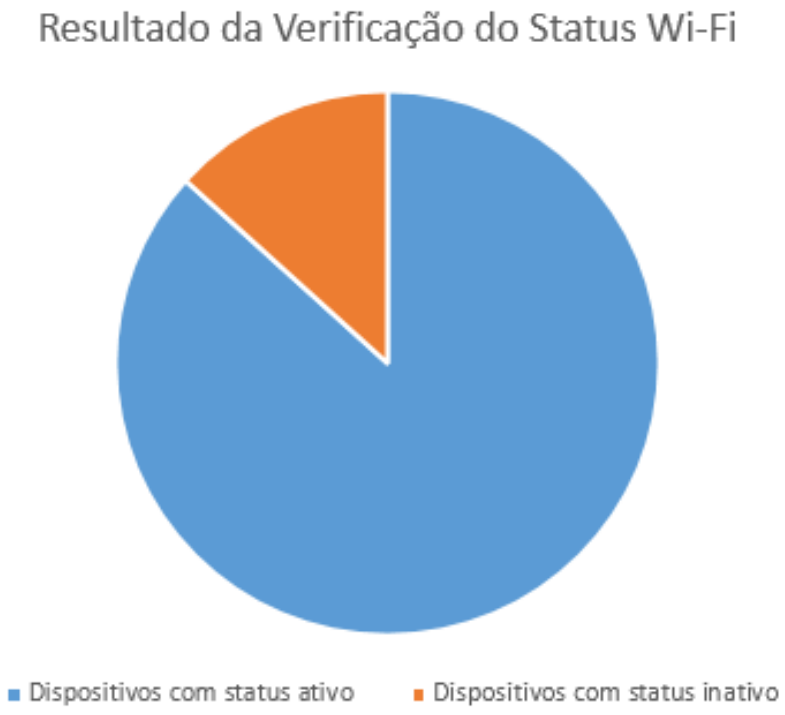
para que fossem avaliados os resultados obtidos, em relação à verificação de alguns dos pontos sugeridos pela cartilha.

Partindo do princípio que a aplicação em sua versão atual contempla cinco verificações de sugestões contidas na cartilha, coube a estes testes a busca por vulnerabilidades a partir da verificação do *status* da *Wi-Fi*, GPS e *bluetooth*, além da verificação de o aparelho possuir como modo de bloqueio de tela um dos modos mais seguros, sugeridos pelo trabalho e pela verificação de o dispositivo estar ou não com a última versão do Android disponível para o mesmo, instalada.

Foram priorizados usuários que não tivessem grandes conhecimentos sobre segurança e tecnologia da informação, pois eles são o alvo maior do trabalho.

Obteve-se como resultado que, dos dispositivos avaliados, 86.7% estavam com o *status* da Wi-Fi ativo durante o teste. A Figura 9 ilustra esse resultado.

Figura 9. Resultado da Verificação do Status da Wi-Fi.



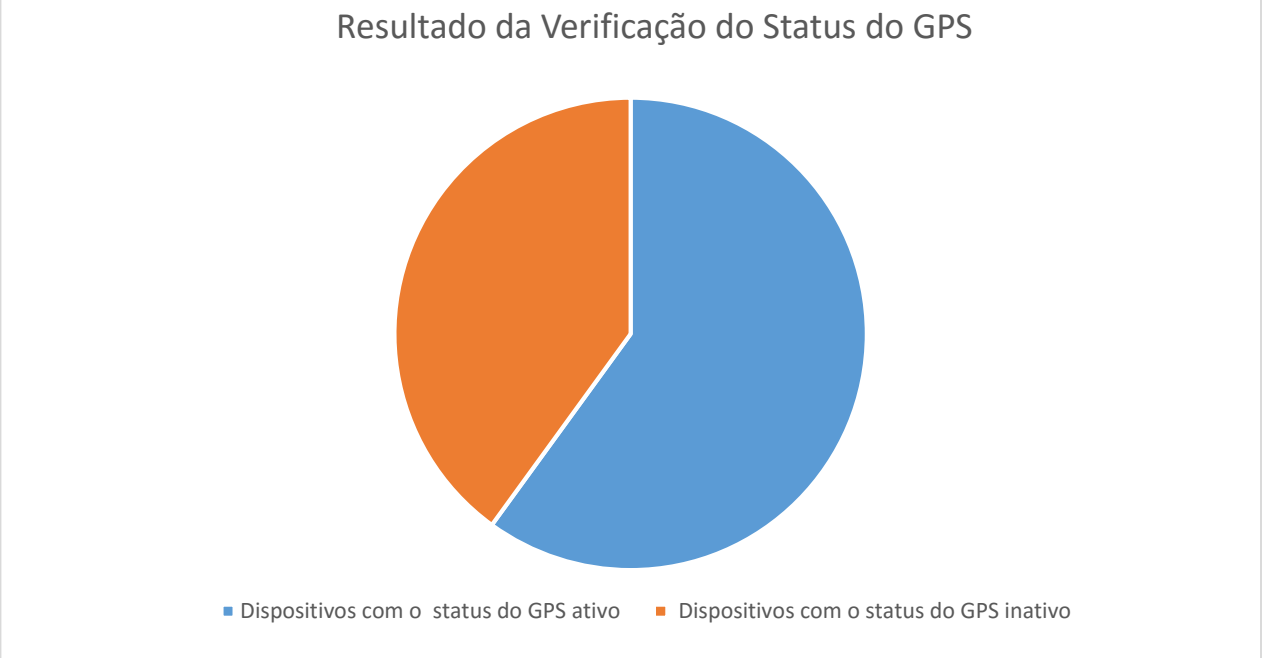
Fonte: Elaborada pela autora.

Ainda analisando os 86.7% dos *smartphones* com o *status* da *Wi-Fi* ativo, observou-se que no momento do teste, apenas 67% dos usuários estavam conectados a

alguma rede e fazendo uso dessa conexão. Os restantes 33% afirmaram estar com a rede ativa pelo fato de esquecer/não saber da necessidade de desativá-la após seu uso.

Em relação ao GPS, 60% dos dispositivos estavam com essa funcionalidade ativa. Fator que eleva a insegurança do dispositivo pois, conforme já exposto nesse trabalho, ao ativar o serviço de geolocalização o usuário estará vulnerável a ser localizado mesmo não havendo consentimento por parte do mesmo. A Figura 10 ilustra a diferença entre dipositivos com GPS ativo e inativo.

Figura 10. Resultado da Verificação do Status do GPS



Fonte: Elaborada pela autora.

Ainda como resultado dos testes analisou-se que 26,7% dos dispositivos possuíam bloqueio de tela classificados como um dois mais seguros por este documento: senha ou reconhecimento de impressão digital.

Quanto ao *bluetooth¸ em* apenas 13.3% dos dispositivos essa funcionalidade se encontrou ativa. Em nenhum dos dispositivos estava sendo realizada trasnferência de dados. Ou seja, constatou-se mais uma vez que ainda há usuários que deixam ativas conexões sem fio sem que esteja fazendo uso da mesma.

No que se refere à atualização da versão do Android, pelo fato de a versão mais recente até então (versão 6) não estar totalmente disponível, nenhum dos dispositivos a possuía. Porém, apenas 40% dos usuários estavam cientes da necessidade de verificar a versão do Android em seu dispositivo para uma possível atualização. Há casos em que a versão mais atual do Android não é compátivel ao dispositivo. Portanto, pede-se que cada usuário busque pela versão mais recentemente disponibilizada para seu dispositivo.

Ao fim do teste conclui-se que valores altos e recorrentes de riscos como, por exemplo, a quantidade de dispositivos com *Wi-Fi* ativa e GPS ativo, reiteram a relevância da contribuição da solução proposta para a sociedade. Acredita-se que com a aquisição da cartilha e a instalação do aplicativo, o usuário estará mais apto a realizar em seu dispositivo a mitigação de riscos de segurança. Pois, a partir da execução da aplicação e da prática das sugestões contidas na cartilha, será de conhecimento do mesmo quais ações tomar/evitar para um uso mais seguro.

5.3 ANÁLISE COMPARATIVA COM A CARTILHA PARA DISPOSITIVOS MÓVEIS PROPOSTA PELO CERT.BR

A nível de informação inicial, tem-se que a cartilha desenvolvida pelo CERT.br teve o propósito e promover a conscientização sobre o uso seguro da *internet*, quando no ano 2000, foi identificada a necessidade da existência de um guia que contivesse informações sobre segurança que e pudesse ser usado como referência pelos diversos setores usuários de Internet. Foi então lançada a Cartilha de Segurança para Internet Versão 1.0. Apenas em 2005, na Versão 3.0, foram incluídos tópicos específicos sobre segurança em dispositivos móveis. Em 2012 foi verificada a necessidade de revisão geral do documento, o que deu origem à versão 4.0. Com o uso crescente da Internet e das redes sociais, impulsionado principalmente pela popularização dos dispositivos móveis e facilidades de conexão, constatou-se a necessidade de abordar novos conteúdos e agrupar os assuntos de maneira diferente (CERT.BR., 2012).

A cartilha do CERT.br sugeriu aos usuários opções que requerem um maior nível de conhecimento técnico, como por exemplo, sugeriu-se que sejam evitados dispositivos que tenham sido ilegalmente desbloqueados (*jailbreak)*. Mas, não foram encontradas na cartilha maneiras possíveis pelas quais o usuário podem realizar essa verificação.

Em se tratando do uso de aplicativos, a cartilha indicou a instalação de antivírus e *firewall* pessoal. Mas, novamente introduziu ações a serem realizadas inclusive por leitores que podem não saber de que se trata, fazendo com que houvesse a probabilidade de a informação não ser realizada por falta de conhecimento. A configuração de um *firewall, por exemplo,* não se enquadra como funcionalidade de fácil entendimento para usuários comuns.

Foi sugerido também que o usuário possuísse certa cautela no que se refere à permissão de dados pessoais aos aplicativos, mas não foi informado ao usuário a partir de que ação o controle dessa permissão é alcançado.

Fez-se presente a ideia do bloqueio na tela inicial, porém, não foram encontrados registros capazes de informar para os leitores quais dos métodos já existentes são os mais seguros, e estão mais aptos a exercer de melhor maneira a função de evitar que pessoas não autorizadas tenham acesso às informações contidas no dispositivo.

Seria interessante a existência da especificação de cada item da cartilha, ou pelo menos dos que exigem mais conhecimento técnico, para que houvesse o entendimento, e com isso, a tomada da decisão proposta pelo documento. Pois, pelo fato de se tratar de um documento público, um dos alvos pode ser representado pelos usuários leigos em segurança e tecnologia da informação.

Em relação ao acesso a redes, a cartilha apenas sugeriu que esses fossem desabilitados quando não utilizados. Não foi explicado o motivo para a necessidade dessa tomada de decisão, como também, não foi contemplada possibilidade de o usuário estar utilizando seu dispositivo como roteador *Wi-Fi* (*hotspot)*. A importância da presença desse item se dá pelo fato de, caso em um dispositivo esteja ativa a função de *hotspot*, é essencial a existência e permanência de uma senha para controle de acesso a essa rede compartilhada. Pois, usuários má intencionados podem conseguir acesso aos dados do dispositivo roteador, sem que sejam autorizados e/ou descobertos.

A cartilha do CERT.br enfatizou ainda o caso de o usuário ter sido vítima de roubo ou perda, ou apenas que ele tenha se desfeito de seu dispositivo. Relatou a necessidade da remoção dos os dados presentes no aparelho.

Como adendo, tem-se que na cartilha em análise não está presente a sugestão de o usuário ativar o recurso de Verificar Aplicativos. Essa funcionalidade verifica periodicamente os aplicativos instalados e caso um aplicativo seja identificado como prejudicial, o verificador pode recomendar a desinstalação, ou ainda, remover o aplicativo julgado como perigoso.

Na cartilha proposta a opção de ativar o verificador de aplicativos é uma das sugestões propostas. Sua relevância se dá pelo fato de estar diretamente relacionada à tomada de decisão a partir do usuário, como também, por ter sido um dos principais meios de combater os riscos de segurança, ainda segundo o relatório da Google.

Portanto, conclui-se que a cartilha desenvolvida por este trabalho possui diferencial a partir do pressuposto que visa atender aos usuários comuns, identificados como usuários sem grandes conhecimentos de segurança e tecnologia da informação. Pois, para cada item sugerido, há a explicação e o motivo de cada tomada de decisão. Como também, diferencia-se pela adição de novas boas práticas, que foram resultantes de estudos que tiveram como referencial teórico documentos escritos posteriormente à publicação das cartilhas, também tidas como referência.

6 CONSIDERAÇÕES FINAIS

Este trabalho objetivou a proposta de uma estratégia integrada, composta por uma cartilha e uma aplicação, para suporte a melhoria das decisões de configuração do usuário de dispositivos móveis Android.

A cartilha desenvolvida é composta por dez sugestões de boas práticas que são resultados das análises dos mais reincidentes ataques de segurança aos dispositivos móveis com o sistema operacional Android, e que são diretamente ligados a questões de má configuração por parte do usuário.

Com a finalidade de avaliar a necessidade da aplicação e das sugestões nela descritas, foram realizadas entrevistas com usuários comuns. 67% desses usuários afirmam ter preocupação com a segurança de seus dispositivos móveis, mas 80% afirmam não ler as permissões requeridas por um aplicativo em seu processo de instalação. Portanto, embora mais da metade dos entrevistados tenha afirmado estar preocupada com a segurança de seus dispositivos móveis, ações para buscar a garantia dessa segurança e a redução da vulnerabilidade a ataques não é do conhecimento de todos. Desta forma, as entrevistas apresentam indícios interessantes relacionados a importância da cartilha aqui apresentada.

Durante o trabalho foi também desenvolvida uma aplicação cuja finalidade é verificar a adoção das boas práticas sugeridas na cartilha. A aplicação e a cartilha tiveram uma boa aceitação pelos entrevistados. Todos os entrevistados afirmaram ter interesse em visualizar a cartilha e ter a aplicação instalada em seus dispositivos móveis. Pois, após testes realizados com usuários e seus dispositivos, verificou-se a muitas das boas práticas encontradas na cartilha não vêm sendo seguidas pelo usuário.

Foi ainda resultado do estudo sobre o tema proposto a publicação de três trabalhos: Riscos de Segurança na Computação Móvel (BIONE, T.A, LINS, F.A.A, 2013), Mitigação de Riscos de Segurança em Ambientes Android Baseada na Melhoria das decisões de Configuração (BIONE, T.A, LINS, F.A.A, 2014) e Proposta de Cartilha Pedagógica para Melhoria de Decisões de Segurança do Usuário de Dispositivos Móveis (BIONE, T.A., LINS F.A.A, 2015).

6.1 TRABALHOS FUTUROS

Como trabalho futuro, cita-se a continuação da implementação da aplicação. Atualmente, a aplicação verifica apenas alguns pontos descritos na cartilha. O intuito é de verificar todos os pontos listados na cartilha. A partir da finalização da implementação, o intuito é disponibilizar a aplicação em lojas virtuais oficial para que a população em geral tenha acesso a mesma.

APÊNDICE A – CARTILHA SOBRE SEGURANÇA EM DISPOSITIVOS MÓVEIS

Figura 11. Anverso da Cartilha Sobre Segurança em Dispositivos Móveis

Esta cartilha tem como objetivo auxiliar os usuários de dispositivos móveis com o sistema operacional Android no que se diz respeito a tomada de decisões de configurações, com a finalidade de reduzir os riscos de segurança.

Portanto, algumas boas práticas são descritas ao longo desta cartilha. Sugere-se que todas sejam analisadas, e na medida do possível, seguidas.

Boa leitura!

1) Evitar Dispositivos que Tenham Sido Ilegalmente Desbloqueados.

A esse desbloqueio denomina-se *root*, e ele pode ser realizado em qualquer dispositivo. Alguns usuários ativam o modo *root* para ter maior permissão diante o seu dispositivo. Porém, ao ativar, o usuário pode deixar o sistema mais vulnerável. Pois, caso haja invasão por algum software malicioso, este terá mais controle sobre o sistema, proporcionado pelo modo *root*.

2) **Manter a Versão do Android e a Versão do Aplicativo Sempre Atualizadas.**

Sempre que uma vulnerabilidade de segurança é descoberta, é disponibilizada uma atualização do *software* com a finalidade de corrigir o erro. Existe opção de deixar que o dispositivo e as aplicações sejam atualizados automaticamente. A sugestão é que essa opção seja ativa, ou que seja função do usuário verificar frequentemente versões atualizadas para seu sistema operacional, ou para seus aplicativos. No ano de 2014 o Android desenvolveu 79 *patches* (programas de computador criado para atualizar ou corrigir um *software*) de segurança.

3) **Ser Cuidadoso ao Instalar Aplicações Através de Sites Externos à Loja Oficial do Androide.**

Aplicativos enviados à Google Play são analisados e classificados quanto à segurança. Essa análise é feita a partir de um sistema chamado *Bouncer*, que verifica o APP e detecta comportamentos suspeitos. O risco de se instalar um aplicativo nocivo dentro da loja oficial é inferior ao risco de aplicações instaladas a partir de sites terceiros, pois, a instalação de aplicativos a partir de lojas externas não é verificada pelo sistema *Bouncer*.

4) **Manter Interfaces de Comunicação como *Bluetooth*, *Wi-fi* e Redes Móveis Habilitadas Apenas Quando Necessário.**

Sugere-se que se deixe apenas ativas as interfaces que estejam em uso. É possível ter acesso a dados do dispositivo através de conexão via redes sem fio. A priori, essa comunicação entre dispositivos se dá apenas com autorização dos dispositivos envolvidos. Porém, com a finalidade de acesso a dados pessoais sem que haja autorização do proprietário, é possível a intercepção de dados a partir da execução de *softwares* maliciosos que são capazes de prover a conexão entre dispositivos sem que o proprietário do dispositivo "vítima" seja notificado.

5) **Não Seguir *Links* Recebidos por Meio de Mensagens Eletrônicas.**

Sugere-se que evite clicar em *links* recebidos através de mensagens eletrônicas pois, é comum a utilização desses *links* para ações com fins maliciosos. Há a possibilidade de, ao clicar em *links* desconhecidos, o usuário fornecer sem consentimento, informações confidenciais. Ainda que que tenha sido enviada por alguém conhecido/de confiança, o ideal é que se confirme o envio do *link*. Muitas vezes nem o próprio remetente sabe do envio, uma vez que anteriormente já foi vítima do ataque, o que o faz repassar o conteúdo automaticamente para os seus contatos.

6) Inserir um Bloqueio de Tela.

O primeiro contato com o dispositivo é a partir da tela de bloqueio. Quanto mais protegida estiver a tela, menor é a probabilidade de o agente ter acesso às informações contidas no dispositivo móvel. O Android permite ao usuário cinco modos de bloqueio de dela: Reconhecimento facial, padrão de desenho, PIN, senha e reconhecimento de impressão digital. Recomenda-se que o proprietário faça de um dos modos oferecidos pelo sistema operacional, o seu controle de acesso. Os meios mais seguros são o reconhecimento de impressão digital ou a senha.

7) **Antes de Instalar uma Aplicação, Ler as Permissões que a Mesma Requisita Ter Acesso.**

Todos os aplicativos ao serem instalados em um dispositivo com a plataforma Android possuem uma lista de permissões. É de grande importância que o usuário leia essas informações para ter conhecimento de quais informações cada aplicativo terá acesso. Algumas aplicações requerem acesso a permissões que vão além das requeridas para que sejam executadas suas atividades. Quando isto ocorre, pode se tratar de um aplicativo malicioso, pois, quando o acesso é permitido, o aplicativo tem total acesso às informações, podendo o agente utilizar desses dados para fins quaisquer.

8) Remover Os Dados Dispositivo Em Caso De Perda/Roubo.

A ameaça de maior probabilidade de ocorrência é o extravio do dispositivo, principalmente quando em conjunto são inseridas aplicações maliciosas. Portanto, em caso de perda ou roubo de seu dispositivo, sugere-se que seja feita a limpeza remota, que é responsável por apagar todos os dados do aparelho e redefinir a configuração original. Para que

Fonte: Elaborado pela autora.

Figura 12. Verso da Cartilha Sobre Segurança em Dispositivos Móveis.

a limpeza remota seja realizada, é preciso que o usuário tenha associado ao seu dispositivo, uma conta da Google, e que através de um navegador da WEB acesse o site admin.google.com, faça o *login* e opte por gerenciamento de dispositivos móveis, onde deverá ser escolhido o dispositivo no qual será efetuada a limpeza remota.

9) **Ativar o serviço de Verificação de Aplicativos.**

Pelo fato de o Android ser uma plataforma que permite a instalação de aplicativos originados de lojas externas à loja oficial, a Google analisou a necessidade de maior controle dos dispositivos. Aos aplicativos da loja oficial, foi adicionada a varredura a partir do *Bouncer*. Portanto, a Google desenvolveu um sistema chamado Verify Apps com o intuito de realizar a varredura nos dispositivos para buscar por vulnerabilidades em aplicativos externos a sua loja oficial. Sugere-se, no entanto, a ativação do serviço de verificação de aplicativos para que seja realizada a busca de aplicativos com comportamento possivelmente malicioso.

10) **Não Permitir a Instalação de Aplicativos a Partir de Fontes Desconhecidas.**

Para haver maior controle de quais aplicativos estão sendo instalados, os dispositivos com o sistema operacional Android vêm configurado de modo a não permitir instalações originadas de fontes desconhecidas. Porém, basta o usuário acessar o menu de configurações, que terá acesso a habilitar a permissão da instalação. Essa prática não é recomendada pelo fato de nas lojas oficiais haver a verificação dos aplicativos com a finalidade de buscar por comportamentos maliciosos antes de os mesmos serem instalados no dispositivo. O mesmo não ocorre nas aplicações de fontes externas, que só serão analisadas após a instalação, caso o *Verify Apps* esteja ativo.

11) Ao ativar o roteador de *WiFi (hotspot)* manter uma senha para controle de acesso à rede.

É possível tornar um dispositivo móvel em um roteador *WiFi*. Ao acessar o menu de configurações do dispositivo, há a funcionalidade que permite que o usuário compartilhe sua rede e permita que outros dispositivos tenham acesso à internet, por exemplo, a partir de seu aparelho. O risco ao tornar ativa essa funcionalidade se dá em casos em que o acesso à rede roteada não utiliza um controle de acesso através do uso de senha. Pois, pessoas má intencionadas podem entrar nessa rede e interceptar dados sem que o proprietário da informação tenha conhecimento do ocorrido. Atualmente, o sistema Android já fornece ao usuário uma senha quando o mesmo ativa o modo roteador em seu dispositivo. Sugere-se que essa senha seja mantida, e caso haja a desconfiança de que outros dispositivos desconhecidos estão tendo acesso à rede, sugere-se que a mesma seja trocada.

Fonte: Elaborado pela autora.

REFERÊNCIAS

BRAGA, A. M. *et al.* Introdução à Segurança de Dispositivos Móveis Modernos – Um Estudo de Caso em Android. *Minicursos do XII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, p. 52–100, 2012.

BIONE, A.A., LINS, F.A.A. Riscos de Segurança na Computação Móvel. p. 1-3, 2013

BIONE, A.A., LINS, F.A.A. Mitigação de Riscos de Segurança em Ambientes Android Baseada na Melhoria das Decisões de Configuração. p. 1, 2014

BIONE, A.A., LINS, F.A.A. Proposta de cartilha pedagógica para melhoria de decisões de segurança do usuário de dispositivos móveis. p. 1, 2014

BIZAGI. *Business Process Management and workflow software*, 2015. Disponível em: <https://www.bizagi.com>.

BRITO JÚNIOR, Á. F. DE; FERES JÚNIOR, N. A utilização da técnica da entrevista em trabalhos científicos. *Evidência: Olhares e Pesquisa em Saberes Educacionais*, v. 7, n. 7, p. 237–250, 2011. Disponível em: <http://www.uniaraxa.edu.br/ojs/index.php/evidencia/article/view/200/186>.

CAIS/RNP. Cartilha de segurança em Dispositivos Móveis. . -: RNP, 2012

CALLAHAM, J. *Galaxy Nexus Android 4.0 Face Unlock broken by picture*. Disponível em: <http://www.neowin.net/news/galaxy-nexus-android-40-face-unlock-broken-by-picture>. Acesso em: 23 maio 2015.

CAMPOS, A. SISTEMAS DE SEGURANÇA DA INFORMAÇÃO. 2 ed. Florianopolis: Visual Books, 2007.

CERT.BR. Cartilha de Segurança para Internet: Fascículo Dispositivos Móveis. . -: cert.br. 2012

DAVI, L. *et al. Privilege Escalation Attacks on Android.pdf*. . Bochum, Germany: [s.n.], 2010.

DI CERBO, F. *et al.* Detection of malicious applications on android OS. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, v. 6540 LNCS, p. 138–149, 2011.

ENCK, W. *et al.* A Study of Android Application Security. *USENIX security …*, n. August, p. 21–21, 2011. Disponível em: <http://www.usenix.org/event/sec11/tech/slides/enck.pdf>.

FARMER, R. A Brief Guide to Android Security. p. 1–16, 2011.

FERRI-BENEDETTI, F. *WHICH SOFTWARE IS THE SAFEST?* Disponível em: <http://mverttech.weebly.com/home/which-software-is-the-safest-by-fabrizio-ferri-benedetti>. Acesso em: 15 jun. 2015.

GOOGLE. *Android Developer Tools | Android Developers*. Disponível em: <http://developer.android.com/tools/help/adt.html>. Acesso em: 15 jul. 2015.

GOOGLE. *Android Security 2014 Year in Review*. . [S.l: s.n.], 2014. Disponível em: <https://static.googleusercontent.com/media/source.android.com/en//devices/tech/security/reports/Google_Android_Security_2014_Report_Final.pdf>.

MALM, S.; OSBORNE, L. *Mobile phone companies can predict future movements of users by building a profile of their lifestyle*. Disponível em: <http://www.dailymail.co.uk/sciencetech/article-2190531/Mobile-phone-companies-predict-future-movements-users-building-profile-lifestyle.html>. Acesso em: 10 abr. 2015.

MOHINI, T.; KUMAR, S. A.; NITESH, G. Review on Android and Smartphone Security. v. 1, n. 6, p. 12–19, 2013.

NAMESTNIKOV, Y.; MASLENNIKOV, D. *Kaspersky Security Bulletin 2012. The overall statistics for 2012*. Disponível em: <https://securelist.com/analysis/kaspersky-security-bulletin/36703/kaspersky-security-bulletin-2012-the-overall-statistics-for-2012/>. Acesso em: 20 maio 2015.

OFICINADANET. *Segurança da informação, conceitos e mecanismos*. Disponível em: <http://www.oficinadanet.com.br/artigo/1307/seguranca_da_informacao_conceitos_e_mecanismos>. Acesso em: 15 jul. 2015.

OH, T. *et al.* Best security practices for Android, BlackBerry, and iOS. *2012 the 1st IEEE Workshop on Enabling Technologies for Smartphone and Internet of Things, ETSIoT 2012*, p. 42–47, 2012.

OLIVEIRA, J. V. DE. *Entrevistas*. . [S.l: s.n.], 2000. Disponível em: <http://w3.ualg.pt/~jvolivei/ep/ep.html>.

ORTHACKER, C. *et al.* Android security permissions - Can we trust them? *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, v. 94 LNICST, p. 40–51, 2012.

ORTIZ, C. E. Understanding security on Android. *IBM - Developer Works*, 2010.

PAULO, B.; KOVACS, U.; MONTEIRO, D. F. portáteis com Windows Mobile Índice. 2006.

PERAKOVIĆ, D.; HUSNJAK, S.; REMENAR, V. Research of security threats in the use of modern terminal devices. *23td International DAAAM Symposium*, v. 23, n. 1, p. 545–548, 2012.

POSTCORE, T. *"TOMA ESSA, FABRICANTES": DESENVOLVEDORES MOSTRAM QUE DETERMINAÇÃO É TUDO - HTC G1 O 1° SMARTPHONE COM ANDROID, RODA O JELLY BEAN*. Disponível em: <http://letsgodroid.blogspot.com.br/2012/08/toma-essa-fabricantes-desenvolvedores.html>. Acesso em: 14 jul. 2015.

REIS, H. T. E. DOS. *Segurança da informação e a Educação a distância*. [S.l: s.n.], 2011.

RODRIGUES, B. S.; CARVALHO, M. A. A. *Segurança da informação no ambiente corporativo. ANAIS DO ENCONTRO DE INICIAÇÃO CIENTÍFICA DAS FACULDADES INTEGRADAS "ANTONIO EUFRÁSIO DE TOLEDO".* Presidente Prudente - SP: [s.n.], 2012.

SIMÕES, F. O. *et al.* Autenticação biométrica multimodal para dispositivos móveis. 2011. Disponível em: <http://www.infobrasil.inf.br/userfiles/Autenticac¸ ˜ao biom´etrica multimodal para dispositivos m´oveis.pdf>.

STACKOVERFLOW. *android - check whether lock was enabled or not - StackOverflow*. Disponível em: <http://stackoverflow.com/questions/7768879/check-whether-lock-was-enabled-or-not>. Acesso em: 14 jul.

STALLINGS, W.; BROWN L. *Computer Security: Principles and Practice.* 2 ed. Pearson, 2011.

SWISHER, K. *Mary Meeker Explains Internet 2012 in 17 Minutes: The Full D10 Interview (Video)*. Disponível em: <http://allthingsd.com/20120612/mary-meeker-explains-internet-2012-in-17-minutes-the-full-d10-interview-video/>. Acesso em: 8 jul. 2015.

TEDESCHI, E. *Segurança no Padrão de Desbloqueio Android*. Disponível em: <http://www.oerick.com/2010/12/21/seguranca-no-padrao-de-desbloqueio-android/>. Acesso em: 13 jul. 2015.

VIASOFT. *Brasileiro é o que mais utiliza tablet para uso profissional, diz Accenture*. Disponível em: <http://www.viasoft.com.br/imprensa/noticia/44/brasileiro-e-o-que-mais-utiliza-tablet-para-uso-profissional-diz-accenture>. Acesso em: 7 jul. 2015.

YANG, J.; CHEN, Z.; DEFINITION, A. Cloud Computing Research and Security Issues. p. 10–12, 2010.

ZHOU, Y.; JIANG, X. Dissecting Android malware: Characterization and evolution. *Proceedings - IEEE Symposium on Security and Privacy*, n. 4, p. 95–109, 2012.