KLEVER REGIS PIRES CAVALCANTI

UMA SOLUÇÃO INTEGRADA PARA A MELHORIA DA SEGURANÇA DE DISPOSITIVOS MÓVEIS BASEADA NA PLATAFORMA *ANDROID*

RECIFE-PE - AGOSTO / 2016

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA APLICADA

Uma Solução Integrada para a Melhoria da Segurança de Dispositivos Móveis Baseada na Plataforma *Android*

Dissertação apresentada ao Programa de Pós-Graduação em Informática Aplicada como exigência parcial à obtenção do título de Mestre.

Orientador: Prof. Dr. Fernando Antônio Aires Lins

RECIFE-PE – AGOSTO/2016

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas da UFRPE
Biblioteca Central, Recife-PE, Brasil

C376s Cavalcanti, Klever Régis Pires
Uma solução integrada para a melhoria da segurança de dispositivos móveis baseada na plataforma android / Klever Régis Pires Cavalcanti . – 2016.
73 f. : il.

Orientador: Fernando Antônio Aires Lins.
Dissertação (Mestrado) – Universidade Federal Rural de Pernambuco, Programa de Pós-Graduação em Informática Aplicada, Recife, BR-PE, 2016.
Inclui referências e apêndice(s).

1. Dispositivos móveis 2. Segurança em dispositivos móveis 3. Android I. Lins, Fernando Antônio Aires, orient. II. Título

CDD 004

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA APLICADA

Uma Solução Integrada para a Melhoria da Segurança de Dispositivos Móveis Baseada na Plataforma *Android*

KLEVER RÉGIS PIRES CAVALCANTI

Dissertação julgada adequada para obtenção do título de Mestre em Informática Aplicada, defendida e aprovada por unanimidade em 19/08/2016 pela Banca Examinadora.

Orientador:

═══════════════════════════════════

Prof. Dr. Fernando Antônio Aires Lins

Universidade Federal Rural de Pernambuco

Banca Examinadora:

═══════════════════════════════════

Prof. Dr. Nelson Souto Rosa

Universidade Federal de Pernambuco

═══════════════════════════════════

Prof. Dr. Erica Sousa

Universidade Federal Rural de Pernambuco

═══════════════════════════════════

Prof. Dr. Ricardo Cavalcante

Universidade Federal Rural de Pernambuco

Dedicatória

Dedico este trabalho a minha esposa Andrea, e as minhas filhas Laura e Luana, pelo tempo que deixamos de estar juntos. Aos meus pais, Lurdes e Kleber, a eles todos os créditos.

AGRADECIMENTOS

Em primeiro lugar a Deus, por me permitir ter chegado até aqui, e por me dar forças nos momentos difíceis.

Em segundo, àquela que está sempre ao meu lado, em todos os momentos e que me ajuda bastante. Obrigado esposa por sempre estar ao meu lado e ter me ajudado de todas as formas e aos meus pais por tudo que fizeram e fazem por mim, realmente sem eles não estaria realizando este sonho.

Agradeço ao meu orientador, professor e amigo Fernando Antônio Aires Lins que realmente caiu do céu, uma pessoa realmente humana que soube entender as dificuldades que a gente passa a cada dia, trabalho e nascimento das minhas filhas, mas sabe cobrar de uma maneira sutil e eficaz. Agradeço muito pelas conquistas, incentivos e generosidade.

Obrigado também a todos que diretamente e indiretamente ajudaram muito nessa empreitada, ao professor Gilberto Cysneiros pelas aulas de *Android* outro ser humano maravilhoso, a sabedoria e o jeito de conduzir as coisas do professor e coordenador Tiago Ferreira, a professora Ceça uma amigona e o professor Rodrigo Assad.

Obrigado aos meus amigos que fiz durante o mestrado, tenho muita sorte por ter encontrado pessoas tão maravilhosas e especiais, Nielson sempre disposto a ajudar, Hélder pela força, ajuda e a todos outros que ajudaram bastante.

Epígrafe

“Ninguém pode voltar atrás e fazer um novo começo. Mas qualquer um pode recomeçar e fazer um novo fim”.

Chico Xavier.

RESUMO

Atualmente, os dispositivos móveis já fazem parte da vida dos usuários, principalmente para verificar e-mails, acessar as redes sociais, fazer pagamentos, acessar contas bancárias ou navegar na *Internet*, e também pela necessidade de estarem conectadas 24 horas por dia. Adicionalmente, o número de vírus e ataques por pessoas mal intencionadas aos dispositivos móveis cresce a cada dia, fruto principalmente de ações comportamentais dos usuários que não configuram corretamente o dispositivo móvel, deixando-o vulnerável. Ações como: não colocar senha na tela inicial, não criptografar o cartão de memória, não utilizar um antivírus, baixar aplicativos não oficiais e outros são exemplos da má configuração do usuário. Portanto, com o intuito de auxiliar o usuário a configurar corretamente o seu dispositivo móvel, este trabalho objetiva a elaboração de uma estratégia para a minimização de riscos de segurança em dispositivos móveis. A estratégia consiste no desenvolvimento de uma solução denominada MSC- *Mobile Security Check*, que tem como objetivo ajudar o usuário na busca de más configurações do dispositivo móvel em termos de segurança com base em 16 itens pré-configurados em relação à má configuração. Esses 16 itens foram escolhidos tendo como base pesquisas científicas, artigos e cartilhas de segurança relacionadas com problemas de segurança advindos de má configuração por parte do usuário final. Esta solução foi implementada baseada no sistema operacional *Android* e está disponível na loja virtual deste ambiente. A avaliação da solução proposta mostrou que, mesmo com usuários com bom nível de conhecimento de segurança em dispositivos móveis, é comum a existência de diversas vulnerabilidades de configuração, e a solução proposta atua diretamente para o levantamento dessas brechas e posterior divulgação ao usuário final. Desta forma, o usuário está apto a tomar medidas corretivas para diminuir os riscos de segurança associados ao uso do dispositivo móvel.

Palavras-chave: Dispositivos móveis, Segurança em dispositivos móveis, *Android*, configurações de usuário.

ABSTRACT

Every day, mobile devices are already part of the lives of users, mainly to check emails, access social networks, make payments, access bank accounts or surf the Internet, and also by the need to be connected 24 hours a day. In addition, the number of viruses and attacks by malicious people to mobile devices grows every day, mainly due to behavioral actions of users who do not properly configure the mobile device, leaving it vulnerable. Actions such as to: do not put password on your home screen, do not encrypt the memory card, do not use an antivirus, do not download unofficial applications and others are examples of risky user configuration. Therefore, in order to support the user in the properly configuration of your mobile device, this work aims to propose a strategy to minimize security risks on mobile devices. This strategy is focused on the development of a solution called MSC Mobile Security Check, which aims to help the user in search of risky settings in the mobile device in security terms, and is based on 16 pre-configured items related to common misconfigurations. These 16 items were chosen based on scientific research, security articles and books related to security issues arising from risky configuration by the high-level user. This solution was implemented based on the *Android* operating system and is available on its associated virtual store. The evaluation of the proposed solution has shown that even with users with high level of security knowledge on mobile devices, it is common to find several configuration risks, and the proposed solution works directly for the presentation of these risks and subsequent notification to the high-level user. After that, the user is able to take corrective measures to reduce these security risks of the mobile device.

Keywords: smartphone, security on mobile devices, *Android*, user settings.

LISTA DE ILUSTRAÇÕES

Figura 5.1- Tipo de bloqueio dos usuários TI 57

Figura 5.2- Tipo de bloqueio dos usuários sem conhecimento profundo de TI. 57

Figura 5.3- Comparativo das avaliações 58

LISTA DE TABELAS

Tabela 4.1- Estudo comparativo dos itens presentes nas referências básicas. 36

Tabela 4.2- Os 16 itens da solução MSC 42

Tabela 4.3 - Quantificação dos itens de Segurança 44

Tabela 4.4- Itens de segurança com seu respectivo nível de gravidade..... 45

Tabela 5.1- Percentual de má configuração nos *smartphones* avaliados..... 55

Tabela 5. 2- Nível de entendimento dos usuários 56

LISTA DE ABREVIATURAS, SIGLAS E SÍMBOLOS

API - Interface de Programação da Aplicação

AVG - *Antivírus Guard*

CAIS/RNP- Centro de Atendimento a Incidentes da Rede Nacional de Ensino e Pesquisa.

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

BYOD- *Bring Your Own Device*

GPS - *Global Positioning System*

IOS - *Iphone Operating System*

JDK- *Java Development Kit*

MSC - *Mobile Security Check*

NET - *Network*

NIST- *National Institute of Standards and Technology*

P2P- *Peer to Peer*

PIN - *Personal Identification Number*

PMBOK - *Project Management Body of Knowledge*

RAM - *Random Access Memory*

SBSEG - Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais

SMS - *Short Message Service*

SSL - *Secure Socket Layer*

TI- Tecnologia da Informação

UFRPE - Universidade Federal Rural de Pernambuco.

WAP - *Wireless Application Protocol*

Web – Teia ou Rede

WEP - *Wired Equivalent Privacy*

WI-FI - *Wireless Fidelity*

WPA -*Wi-Fi Protected Access*

SUMÁRIO

1 INTRODUÇÃO 14

1.1 OBJETIVO GERAL 15

1.2 OBJETIVOS ESPECÍFICOS 16

1.3 DEFICIÊNCIAS DO ESTADO DA ARTE 16

1.4 SOLUÇÃO PROPOSTA 18

1.5 ESTRUTURAÇÃO DO DOCUMENTO 19

2 CONCEITOS BÁSICOS 20

2.1 ATRIBUTOS FUNDAMENTAIS DE SEGURANÇA 20

2.2 ARQUITETURA DA PLATAFORMA ANDROID 21

2.3 SEGURANÇA NO ANDROID 21

2.4 SEGURANÇA EM COMPUTAÇÃO MÓVEL 22

2.4.1 Perda do dispositivo Móvel 22

2.4.2 Comunicação Insegura 22

2.4.3 Uso de Programas de Fontes Suspeitas 23

2.4.4 Vulnerabilidades no desenvolvimento de aplicativos móveis 24

2.4.5 Má configuração do usuário 25

2.5 CARTILHAS E GUIA DE SEGURANÇA PARA DISPOSITIVOS MÓVEIS 26

2.6 CONSIDERAÇÕES FINAIS 29

3 TRABALHOS RELACIONADOS 30

3.1 DESCRIÇÃO DAS INICIATIVAS 30

3.2 DISCUSSÃO COMPARATIVA 33

3.3 CONSIDERAÇÕES FINAIS 34

4 MOBILE SECURITY CHECK: UMA SOLUÇÃO PARA A MELHORIA DA SEGURANÇA DE DISPOSITIVOS MÓVEIS *ANDROID* 35

4.1 REQUISITOS 35

4.1.1 Requisitos Funcionais 37

4.1.2 Requisitos não Funcionais 40

4.2 VISÃO GERAL DA SOLUÇÃO 40

4.3 ARQUITETURA DO MSC 47

4.4 IMPLEMENTAÇÃO 48

4.5 CONSIDERAÇÕES FINAIS 52

5 AVALIAÇÃO 54

5.1 AVALIAÇÃO DA EXECUÇÃO DA SOLUÇÃO MSC EM SMARTPHONES 54

5.2 AVALIAÇÃO DO NÍVEL DE ENTENDIMENTO DOS USUÁRIOS SOBRE SEGURANÇA EM COMPUTAÇÃO MÓVEL 56

5.3 AVALIAÇÃO COMPARATIVA 58

5.4 AVALIAÇÃO DO CONSUMO DE ENERGIA DA SOLUÇÃO MSC 59

5.5 CONSIDERAÇÕES FINAIS 60

6 CONCLUSÕES E TRABALHOS FUTUROS 61

6.1 RESULTADOS ALCANÇADOS 61

6.2 TRABALHOS FUTUROS 62

7 REFERÊNCIAS 65

APÊNDICE 71

1 INTRODUÇÃO

A popularização dos dispositivos móveis, como *tablets*, *smartphones* e celulares, têm tornado os dispositivos móveis (especialmente *smartphones*) um alvo em potencial para pessoas mal intencionadas. Usuários comuns estão praticamente conectados 24 horas por dia, seja para checar *e-mails*, acessar redes sociais, *Internet Banking* ou simplesmente navegar na *internet.*

Segundo Grossmann (2015), o Brasil é o sétimo país no ranking global em termos de uso da *Internet*. Outro dado relevante, em termos de segurança, é que até 2016 os *malwares*, que são qualquer código de *software* feito com a intenção de prejudicar dados, dispositivos ou pessoas, chegarão a 20 milhões, e 90% dos vírus afetarão dispositivos móveis *Android* [AVG 2015]. Isto se deve ao fato do *Android* ser o sistema operacional mais utilizado em *smartphones*, fazendo com que o desenvolvimento de códigos maliciosos seja focado nessa plataforma [Storn 2014].

Outro dado interessante é que na América Latina o Brasil concentra sozinho 92,31% de todos os casos de ataques do tipo *ransonware*, que é um tipo de software malicioso (*malware)* com função de “sequestrar” dados de um usuário, ou seja, ele bloqueia o aceso aos arquivos ou sistema e com um pagamento de um valor específico o ataque libera o acesso ao sistema. Esse tipo de ataque aumentou no Brasil devido ao fato das pequenas e médias empresas terem os seus equipamentos mal configurados como: senhas simples ou sem senhas na tela inicial do dispositivo móvel [Romer 2015].

Além do ataque *ransonware*, outros tipos de ataques aos dispositivos móveis que comumente acontecem são: ataque via SMS, ataque via *Bluetooth,* via rede WI-FI pública que um atacante pode interceptar o tráfego (e coletar dados pessoais) ou desviar a navegação para sites falsos [CERT.br 2013], dentre outros, deixando o dispositivo móvel vulnerável a ataques. Além das pequenas e médias empresas terem seus equipamentos mal configurados, muitos usuários também não configuram corretamente o dispositivo móvel e acabam deixando o mesmo com a configuração padrão, não tomando as

devidas precauções de segurança (por exemplo, não colocam senha na tela inicial, deixam o *Bluetooth* ligado, não criptografam o cartão de memória, não instalam antivírus, etc).

A segurança nos dispositivos móveis é uma preocupação constante dos usuários, mas mesmo sabendo dos perigos os mesmos, por exemplo, ainda se conectam a redes WI-FI abertas sem nenhuma segurança e acessam sites de bancos, redes sociais ou e-mails, ficando assim vulneráveis a ataques por pessoas mal intencionadas.

Outro ponto que sugere ainda mais preocupações é o fato das pessoas utilizarem o seu dispositivo móvel em função da empresa, conceito conhecido como BYOD, que vem do inglês *Bring Your Own Device*, que em tradução livre significa “traga seu próprio dispositivo” (D’arcy 2011), aumentando e muito o risco de ter informações importantes ou estratégicas da empresa acessadas por terceiros.

Atualmente existem diversas cartilhas de segurança disponíveis para os usuários, por exemplo, CERT [CERT.br 2013] e CAIS [CAIS/RNP 2012], mas usuários em geral desconhecem e não seguem recomendações básicas e, por esse motivo, surgem abordagens e aplicações para verificação de más configurações, que é o foco principal deste trabalho.

Em resumo, pode-se afirmar que existe atualmente uma lacuna em termos de estratégias para minimização de riscos de segurança em dispositivos móveis Android baseadas na avaliação das decisões de configuração do usuário de alto nível, e especialmente considerando as orientações de segurança sugeridas por diversas referências de segurança de dispositivos móveis importantes [CERT.br 2013] [CAIS/RNP 2012].

1.1 OBJETIVO GERAL

Este trabalho objetiva propor uma solução capaz de minimizar problemas relacionados à má configuração do usuário nos dispositivos móveis. Esta solução deve checar o dispositivo móvel do usuário atrás de más

configurações e posteriormente as apresentar para o usuário tendo em vista possíveis ações corretivas.

1.2 OBJETIVOS ESPECÍFICOS

Os principais objetivos específicos deste trabalho são:

- Diminuir os riscos relacionados à má configuração do usuário no dispositivo móvel através da checagem no dispositivo móvel por eventuais má configuração.
- Alertar para o usuário possibilidades de uma configuração mais segura.
- Disponibilização da solução proposta de forma gratuita para o usuário final em loja virtual.
- Depois da checagem, mostrar qual o nível de segurança em que o dispositivo móvel se encontra (Alto, Médio ou Baixo).

1.3 DEFICIÊNCIAS DO ESTADO DA ARTE

Prover soluções que possam minimizar os riscos de segurança em dispositivos móveis é uma atividade complexa ao se considerar a existência dos vários possíveis tipos de ataques existentes e a vulnerabilidade que os dispositivos móveis sofrem por causa dos usuários não terem o conhecimento devido de como proteger o dispositivo móvel.

Os autores [Jeter 2013] propuseram um aplicativo chamado "*Test Your Phone*", que analisa o comportamento do usuário em relação à segurança na utilização do dispositivo móvel *Android*. Nesta iniciativa, este comportamento é analisado através de questionário, e o dispositivo em si não é avaliado diretamente, mas sim o conhecimento do usuário. A principal contribuição de Jeter é a análise dos dados recolhidos do questionário (ex.: verifica se usuário opta por deixar *Bluetooth* ativado, se o usuário deixa ativado o recurso GPS o

tempo todo, dentre outros). Contudo, a iniciativa não checa o aparelho em si e nem possibilita que o usuário possa verificar e corrigir eventuais falhas.

Outro trabalho que também aborda esta temática é [Braga 2012], que apresenta um estudo de caso com foco nas vulnerabilidades relacionadas às plataformas modernas de dispositivos móveis. O trabalho mostra o problema da má configuração do usuário em relação ao dispositivo móvel, com destaque para a questão da senha de bloqueio da tela inicial e sobre fazer o *rooting* no dispositivo móvel. Contudo, o autor não implementou uma solução prática, que possa ser instalada em dispositivos móveis para a detecção e correção de possíveis problemas de segurança.

Outro trabalho relevante é [Vecchiato 2015], no qual os autores desenvolveram um aplicativo para verificar a segurança das configurações dos usuários nos dispositivos móveis em diferentes níveis, e depois este aplicativo mostra em uma única tela o resultado da verificação em conjunto com a explicação de como corrigir o eventual nível mal configurado. No total são 14 níveis que são verificados automaticamente, e os níveis mais relevantes são: Redes, (informações da rede), Senhas (informações de senhas), Localização (GPS), Aplicativos de Fontes desconhecidas, Antivírus, *Malware* e versão do *Android*. Contudo, a aplicação não foca em outros pontos também importantes, como: verificar se o *Bluetooth* está ligado, verificar se existem aplicativos que consumem muita energia de bateria e que sobrecarregam o sistema do dispositivo. Além disso, um dos níveis, “Localização”, verifica apenas se o GPS está ligado; contudo, outra questão de segurança importante seria verificar aplicativos que utilizam o GPS no *smartphone*.

Em resumo, essas iniciativas abordaram e propuseram iniciativas para a mitigação de problemas de segurança em dispositivos móveis; contudo, existe uma lacuna neste contexto referente a uma iniciativa capaz de verificar diversos itens de má-configuração existentes, onde essa lista de itens deve se basear principalmente na literatura existentes da área, especialmente as chamadas cartilhas de segurança (que serão mais bem abordadas no Capítulo 2).

1.4 SOLUÇÃO PROPOSTA

Tendo em vista as deficiências do estado da arte anteriormente descritas, este trabalho apresenta a solução MSC - *Mobile Security Check*, que visa analisar o dispositivo móvel de modo a encontrar possíveis más configurações por parte do usuário. A solução proposta tem o objetivo de minimizar os riscos de segurança que os dispositivos móveis vem sofrendo nos dias atuais; para isso, após a checagem do dispositivo móvel, a solução mostra os possíveis pontos falhos de segurança e mostra também qual o nível de segurança em que o dispositivo móvel se encontra (Alto, Médio ou Baixo). Com estas informações, cabe ao usuário a decisão de seguir a recomendação de adotar as configurações mais seguras sugeridas. Para tal, a solução é composta de 16 itens de segurança pré-configurados relacionados à má configuração do usuário no dispositivo móvel; estes itens foram elaborados com base em pesquisas por aplicativos similares no Google Play, guias de segurança, artigos e principais cartilhas de segurança em dispositivos móveis, especialmente a do CERT [CERT.br 2014].

A solução MSC se difere de outros trabalhos [Jeter 2013] [Braga 2013] [Thomas 2013] e de aplicativos existentes no *Google Play* como por exemplo DU *Battery Saver* [Studio 2015] por ser direcionada a má configuração do usuário no dispositivo móvel com itens relevantes a segurança do dispositivo baseados em cartilhas oficiais sobre segurança em dispositivos móveis. Além disso, os outros trabalhos que serão mostrados nesta dissertação se baseiam geralmente em estratégias diferentes para uma configuração mais segura, como por exemplo: questionários de segurança respondidos pelos usuários e aplicativos que só fazem análise sobre o tipo de conexão e análise do dispositivo em busca de possíveis vírus. Com isso, a solução MSC de fato checa o dispositivo móvel atrás da má configuração do usuário e recomenda uma configuração mais segura com base em 16 itens presentes nas principais cartilhas de segurança em dispositivos móveis, no guia de orientações do NIST [Souppaya 2013] e do CERT [CERT.br 2013].

De forma resumida, pode-se colocar que a contribuição principal do trabalho é o provimento de uma solução integrada, capaz de procurar e evidenciar possíveis riscos de segurança no dispositivo móvel.

1.5 ESTRUTURAÇÃO DO DOCUMENTO

Além deste capítulo de introdução, o presente trabalho inclui ainda mais cinco capítulos, que são brevemente descritos a seguir:

Capítulo 2: Neste capítulo serão introduzidos conceitos básicos associados a este trabalho. Mais especificamente, são detalhados os aspectos relacionados à confidencialidade, disponibilidade, autenticidade, controle de acesso e também são descritos os principais tópicos das cartilhas de segurança para dispositivos móveis.

Capítulo 3: Neste capítulo, uma discussão sobre os trabalhos relacionados a esta dissertação é apresentada. Esses trabalhos são discutidos e uma avaliação sobre os mesmos é feita.

Capítulo 4: Este capítulo apresenta a solução MSC para checar possíveis más configurações em dispositivos móveis *Android*. Inicialmente, o capítulo apresenta os requisitos funcionais e os requisitos não funcionais, além de mostrar o estudo comparativo dos itens presentes em referências atuais e relevantes da área. Ainda neste capítulo também é apresentado arquitetura e a implementação da solução.

Capítulo 5: Neste capítulo, que busca avaliar o trabalho desenvolvido, foram propostas diversas avaliações para entender e evidenciar com mais clareza as contribuições do trabalho e a importância da solução proposta.

Capítulo 6: Finalmente, este capítulo apresenta as conclusões, resultados alcançados e os trabalhos futuros associados a esta dissertação.

2 CONCEITOS BÁSICOS

Quando se trata de Segurança da Informação, alguns conceitos se apresentam como fundamentais. Esse conceitos são introduzidos na Seção 2.1. Considerando o contexto deste trabalho, que é segurança em computação móvel, também se faz necessário explicitar as principais referências na área, que serão descritas nas Seções 2.2, 2.3, 2.4 e 2.5 e na 2.6 com considerações finais.

2.1 ATRIBUTOS FUNDAMENTAIS DE SEGURANÇA

Quando se trata de segurança, alguns pontos são tidos como fundamentais, e eles são denominados atributos de segurança. Alguns desses atributos serão destacados nesta seção.

Confidencialidade. As informações não devem ser disponibilizadas ou divulgadas a pessoas não autorizadas, entidades ou processos. Por exemplo, informações confidenciais enviadas pela *Internet* (ex.: senha bancária) não devem ser acessados por usuários não autorizados.

Disponibilidade. A informação deve ser acessível e utilizável, mesmo considerando períodos de alta demanda. Por exemplo, a perda de conectividade de um servidor relevante pode afetar a disponibilidade do sistema.

Integridade. Consiste em proteger as informações contra modificação não autorizada, ou seja, sem a permissão dos proprietários de informação.

Autenticidade. Garantir que a informação é realmente da fonte que se declara ser.

Controle de acesso. O objetivo principal é evitar que usuários autenticados, mas não autorizados, tenham acesso ao sistema de uma empresa e suas funcionalidades.

2.2 ARQUITETURA DA PLATAFORMA ANDROID

O *Android* é um sistema operacional e plataforma de código aberto para dispositivo móvel desenvolvido pela *Google* e pela *Open Handset Alliance* [Alliance 2016], uma aliança atualmente formada por 84 empresas, incluindo a Google e empresas líderes no setor tecnológico. A plataforma *Android* é subdividida em cinco camadas principais que são:

1) O *Kernel* que é responsável pelas funcionalidades centrais do sistema, como gerenciamento de memória e de energia, gestão de processos e protocolos de rede otimizado para dispositivos móveis [Android 2016].

2) Bibliotecas Nativas são escritas em C/C++ e provém funcionalidades básicas que podem ser acessadas por desenvolvedores através do *framework* de aplicação [Android 2016].

3) *Android Runtime* Inclui a máquina virtual *Dalvik*, projetada para ser leve e apresentar pouca demanda por memória e processamento, e bibliotecas escritas em *Java*, que são executadas pela *Dalvik* [Android 2016].

4) *Frameworks* de Aplicação são escritos em *Java* e proveem abstrações das bibliotecas nativas, ou seja, classes que atuam em conjunto para dar acesso aos serviços dessas bibliotecas [Android 2016].

5) São os aplicativos com os quais os usuários interagem diretamente. São escritos em *Java* e cada um deles é executado em uma máquina virtual independente [Android 2016].

2.3 SEGURANÇA NO ANDROID

Os recursos de segurança fundamentais que ajudam a construir aplicações seguras incluem:

• O Android aplicação sandbox, é um ferramenta eficaz e simples que isola a execução de programas e seus processos, tornando possível testar as suas operações em um ambiente virtual seguro e controlado.

• Uma estrutura de aplicativo com implementações consistentes de funcionalidade de segurança comum, tais como criptografia e permissões;

• Um sistema de arquivos criptografado que pode ser ativado para proteger dados em dispositivos perdidos ou roubados;

• Permissões concedidas ou negadas pelo usuário para restringir o acesso aos recursos do sistema e dados do usuário.

2.4 SEGURANÇA EM COMPUTAÇÃO MÓVEL

Como visto no capítulo anterior, é inegável o crescimento do uso de dispositivos móveis nos últimos anos. E, junto com este crescimento, pode-se perceber o aparecimento e também crescimento de riscos associados ao uso de dispositivos móveis. Segundo Cavalcanti (2015), estes problemas/riscos podem ser genericamente classificados em: perda do dispositivo móvel; comunicação insegura; uso de programas de fontes suspeita; vulnerabilidades no desenvolvimento de aplicativos móveis; e má configuração do usuário. Essas categorias são detalhadas nas próximas subseções.

2.4.1 Perda do dispositivo Móvel

Quando um dispositivo móvel é perdido, não só o *hardware* está comprometido, mas também a sua informação interna, como por exemplo: fotos, documentos pessoais e configurações. Por exemplo, uma pessoa mal intencionada pode conectar um cabo USB em um *smartphone* e ter acesso a toda a informação que está disponível no dispositivo. Além da exposição de dados internos, uma pessoa mal intencionada de posse dessas informações pode exigir algo em troca. A utilização de senha na tela inicial e ter o cartão de memória criptografado dificultaria a ação de uma pessoa mal intencionada neste tipo de problema [Salutes 2016].

2.4.2 Comunicação Insegura

Pelo grande número de lugares com disponibilidade de acesso a rede WI-FI aberta (Pública), muitos usuários não sabem dos perigos que podem acontecer ao acessarem contas bancárias, redes sociais, *e-mails* e *sites* que

precisem que usuário coloque um *login* e senha. Mais especificamente, três pontos devem ser analisados no contexto de acesso as redes WI-FI públicas: capturas de pacotes em acesso a páginas da *Internet*, a obtenção das credenciais e o sequestro de contas ou acesso de informações. Por exemplo, um usuário que acessa páginas da Web no dispositivo móvel conectado a uma rede WI-FI aberta pode sofrer um ataque, considerando que um usuário malicioso pode verificar a rede aberta e visualizar todo o tráfego que está passando pela rede usando um *snort*, que é um *Sniffer* (programa de captura de pacotes) [CERT.br 2003].

Outra preocupação é se o usuário usar um aplicativo para se conectar ao servidor de correio eletrônico (e-mail) sem usar criptografia, facilitando assim o acesso dos dados de *login* do usuário e/ou dispositivo por possíveis *crackers*.

Sequestro de contas ou acesso de informações não ocorre apenas em computadores pessoais, mas também em dispositivos móveis. Para se proteger contra ataques a dados através de uma rede aberta é importante acessar apenas redes que utilizam algum tipo de criptografia, como: WEP (*Wired Equivalent Privacy*), WPA (*WI-FI Protected Access*) ou WEP (*Wired Equivalent Privacy*), sendo essa última considerada a mais forte em termos de complexidade de criptografia, e é a que vem sendo mais utilizada atualmente [CERT.br 2012].

2.4.3 Uso de Programas de Fontes Suspeitas

Esta categoria se baseia no uso de qualquer programa e aplicativos que são obtidos a partir de fontes suspeitas ou que, pelo menos, não são da loja do *Google Play*. Basicamente, não é recomendado a instalação de aplicativos que não estão nas lojas oficiais por não haver uma verificação de segurança nestes aplicativos; ou seja, não é feita uma varredura por possíveis códigos maliciosos, nos quais podem existir *malwares*. Mesmo assim, um número considerável de usuários faz uso de programas a partir de lojas não oficiais especialmente pela variedade de aplicativos existente, ficando portanto suscetíveis a ataques. Um tipo de ataque conhecido neste contexto é o *botnet*, conhecido como robôs,

cuja função é fazer com que o dispositivo móvel fique programado para realizar tarefas específicas, como fraudar e enganar os usuários. Para se prevenir deste tipo de ataque, o ideal é não fazer *download* de aplicativos de lojas não oficiais e ter no seu dispositivo móvel um antivírus instalado [Braga 2012].

2.4.4 Vulnerabilidades no desenvolvimento de aplicativos móveis

Os programas para plataformas móveis em si podem ser fonte de riscos de ataques, pois é comum a prática de desenvolvedores de aplicações móveis não se preocuparem e nem considerarem os riscos de segurança existentes no projeto das aplicações. Três situações serão destacadas neste contexto: a falta de conhecimento de segurança das equipes de desenvolvimento, ataque indireto e aplicações que requerem permissões avançadas em *Android* [Braga 2012]:

- Conhecimentos de segurança insuficiente da equipe de desenvolvimento do aplicativo é uma grande preocupação, porque muitos aplicativos são desenvolvidos diariamente em sem considerar conceitos básicos de segurança e possíveis ferramentas. Normalmente, os desenvolvedores criam aplicações mais simples, sem se preocupar com a segurança no processo de desenvolvimento [Braga 2012];
- Outro ponto relevante é o ataque indireto, no qual as aplicações *Android* têm alguns certificados previamente gravados por desenvolvedores, dando-lhes acesso especial e privilégios dentro do sistema operacional sem passar pela cadeia do processo de validação do certificado. Por exemplo, a *Adobe* fornece certificados para as suas aplicações. Este processo existe para permitir que outros aplicativos parem de usar o *plug-in Adobe Flash Player* [Player 2016]. Uma situação possível é que um atacante pode validar um aplicativo malicioso com um certificado que a princípio parece ter sido validado pelo código do *Adobe*, mas na verdade não foi validado pelo *Adobe*. Além disso, enquanto o certificado *Adobe* está presente nos certificados do aplicativo, o sistema aceita

código liberado por esta aplicação e infectar de vírus outras aplicações [Novaes 2014];

- Outros riscos estão associados às permissões de aplicativos. Para instalar uma aplicação, é necessário que o usuário aceite algumas permissões. Por exemplo, o usuário pode instalar uma aplicação que requer a permissão dele/dela para usar a câmera, o GPS e outras funções relevantes. Ao fazer isso, o dispositivo móvel do usuário pode tornar-se mais vulnerável, porque este aplicativo pode usar essas permissões para outros fins que não foram mencionadas no processo de instalação. A aceitação do pedido de permissões pode inclusive gerar consequências desagradáveis, como dados pessoais desviados. O problema se torna ainda mais preocupante quando as permissões são combinadas, porque avaliar todas as permissões é desgastante e, geralmente, o usuário simplesmente aceita o pedido sem executar uma revisão significativa. Uma medida preventiva é quando for instalar um aplicativo ler as permissões e tiver cuidado ao instalar um aplicativo que requer muitas permissões, exceto se forem considerados essenciais. Infelizmente, geralmente não é possível aceitar apenas um subconjunto dessas permissões [CAIS/RNP 2012].

2.4.5 Má configuração do usuário

Um número considerável de ataques de segurança ocorre com base na falta de conhecimento do usuário em segurança de dispositivos móveis. Este tipo de usuário geralmente não tem plena consciência do que está sendo feito quando algumas ações são executadas no dispositivo móvel. Com base nisso, esta última categoria é chamada de "Má configuração do usuário", e se concentra em falhas de configuração de usuários comuns que podem produzir riscos de segurança relevantes. Como exemplo, um erro comum de configuração está relacionado à utilização da tecnologia *Bluetooth* e GPS. Muitos usuários utilizam dispositivos móveis e não se preocupam se o *Bluetooth* ou GPS estão ativos (mesmo sem usá-los). Se o *Bluetooth* está

ativo, um invasor pode obter dados confidenciais, como informações do usuário sem o consentimento apropriado. No caso do GPS, deixando-o sempre ativo se torna possível a um atacante localizar a posição atual do usuário e usar essa informação contra o desejo do usuário. Além disso, esses recursos ligados o tempo todo implicam em mais consumo de energia, que tem impacto sobre a disponibilidade do dispositivo [Braga 2012].

Outro exemplo de má configuração ocorre quando o usuário precisa acessar a *Internet* no computador e utiliza à *Internet* do dispositivo móvel. Este procedimento é conhecido como roteador WI-FI portátil ou ancoragem. Se não for configurado corretamente, esta rede é susceptível a ataques, em que um atacante possa ter acesso à informação não autorizada, ou seja, o *smartphone* com a função de roteador ativo pode possibilitar, por exemplo, o roubo de documentos, imagens e arquivos de vídeo, instalação de *software* e roubo de senhas [CAIS/RNP 2012].

Vários problemas de segurança que podem acontecer nos dispositivos móveis foram detalhados nesta seção, e todos podem comprometer a segurança dos dispositivos móveis. Entretanto, o que mais se mostrou alarmante foi a má configuração do usuário, especialmente pela grande quantidade de riscos e más configurações comumente encontradas nos *smartphones* dos usuários comuns (essa quantidade será detalhada em pesquisa realizada no Capítulo 5), e esse fato inspirou o desenvolvimento da solução proposta nesta dissertação.

2.5 CARTILHAS E GUIA DE SEGURANÇA PARA DISPOSITIVOS MÓVEIS

Esta seção mostra as principais cartilhas de segurança em dispositivos móveis que foram a base para elaboração da solução proposta nesta dissertação. Uma cartilha importante é a do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil [CERT.br 2013], que dedica

o seu capítulo 14 para a segurança em dispositivos móveis, elencando os principais itens de segurança que devem ser observados neste contexto.

Outra cartilha importante é a do Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Ensino e Pesquisa [CAIS/RNP 2012], que destaca alguns itens importantes para a segurança dos dispositivos móveis. E por fim um guia de orientações do NIST (*National Institute of Standards and Technology*) [Souppaya *et al* 2013] mostra orientações para a gestão da segurança de dispositivos móveis nas empresas com intuito de ajudar as organizações a gerenciar centralmente a segurança de dispositivos móveis. Essas referências serão brevemente descritas a seguir.

A cartilha de Segurança em dispositivos móveis [CERT.br 2013] está dividida em 6 tópicos e 25 subtópicos de segurança necessários antes de adquirir um dispositivo móvel. Considerando o contexto deste trabalho, destacam-se 7 subtópicos:

1- Restaurar configurações originais de *smartphones* usados. Ao comprar um dispositivo móvel usado, é importante restaurar as configurações originais, ou "de fábrica", antes de começar o seu uso.

2- Evitar adquirir um dispositivo móvel que tenha sido ilegalmente desbloqueado. Conhecido como *jailbreak*, esta prática, além de ser ilegal, pode violar os termos de garantia e comprometer a segurança e o funcionamento do aparelho.

3. Utilizar um antivírus no dispositivo móvel. Ao usar um dispositivo móvel é importante instalar um programa *antimalware,* por exemplo, *Malwarebytes Anti-Malware* [Anti –Malware 2016] antes de instalar qualquer tipo de aplicação, principalmente aquelas desenvolvidas por terceiros.

4. Atualizar regularmente o sistema operacional. É recomendável manter o sistema operacional e as aplicações instaladas sempre com a versão mais recente e com todas as atualizações aplicadas.

5. Evitar a instalação de aplicativos de fonte desconhecida e extensões. Ter cuidado ao instalar aplicações desenvolvidas por terceiros, como

complementos extensões. Procurar usar aplicações de fontes confiáveis e que sejam bem avaliadas pelos usuários.

6. **Verificar se as permissões são coerentes em relação a destinação da aplicação.** Recomenda-se verificar se as permissões necessárias para a execução são coerentes com a destinação da aplicação.

7. **Recomenda-se cautela com aplicativos que usam redes sociais com geolocalização.** Ao entrar em uma rede social é importante ter cuidado com a geolocalização, porque pode comprometer a sua privacidade e com base nela, é possível descobrir a rotina, deduzir informações (como hábitos e classe financeira) e tentar prever os próximos passos ou dos familiares [CERT.br 2013].

Outra importante cartilha é a do Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Ensino e Pesquisa [CAIS/RNP 2012], que destaca a necessidade de se utilizar um antivírus, mas explica que para soluções de segurança não devem tratar apenas de vírus, mas também inibir a instalação de aplicativos que não são de fontes oficiais, impedir a realização do *root* que é ter permissões de administrador do dispositivo móvel, garantir que os cartões de memória sejam criptografados.

A Cartilha CAIS/RNP destaca inclusive um capítulo inteiro para dispositivos móveis *Android*, com ênfase em mostrar como ter acesso as configurações de segurança de qualquer dispositivo móvel *Android*. Para isso, em qualquer dispositivo móvel basta ir na seção “Segurança” de “Configurações do Sistema” (acesso pelo botão Menu), onde se encontram as principais configurações de segurança do sistema operacional como Bloqueio de tela e bloqueio do SIM. No bloqueio de tela de acesso ao dispositivo móvel pode-se escolher a opção “Senha”, que permite a configuração de senhas no dispositivo. No bloqueio do SIM, é possível marcar a opção “Bloquear cartão SIM”, basta clicar em alterar o PIN (*Personal Identification Number*) é um código de segurança que vem definido nos chips das operadoras de telefonia diferente da senha de bloqueio do dispositivo móvel. O PIN já vem definido pela operadora

de telefonia, e assim depois de alterada, somente a pessoa que tiver a senha poderá desbloquear o chip e ter acesso ao dispositivo móvel.

Outra referência relevante é o guia de orientações sobre a segurança de dispositivos móveis nas empresas, produzida pelo NIST (National Institute of Standards and Technology) [Souppaya 2013]. Esta referência destaca um material sobre Orientações para a Gestão da Segurança de Dispositivos Móveis nas empresas com intuito de ajudar as organizações a gerenciar a segurança de dispositivos móveis. É destacado que os dispositivos móveis, como *smartphones* e *tablets*, normalmente precisam suportar múltiplos objetivos de segurança como: confidencialidade, integridade e disponibilidade. Para atingir estes objetivos, os dispositivos móveis devem ser protegidos contra uma variedade de ameaças. Destaca-se ainda a preocupação com rede WI-FI pública, as interfaces de rede de área pessoal sem fio, como *Bluetooth*, e cuidados com ativação do GPS.

2.6 CONSIDERAÇÕES FINAIS

Neste capítulo foram mostrados os atributos fundamentais de segurança como Confidencialidade, Integridade, Disponibilidade e Autenticidade. Na cartilha do CERT foram destacados 7 subtópicos de segurança necessários antes de adquirir um dispositivo móvel. A outra cartilha CAIS/RNP mostrou itens de segurança que são fundamentais para uma configuração correta do dispositivo móvel. A publicação do guia de orientações para a gestão da segurança de dispositivos móveis NIST tem o intuito de ajudar as organizações a gerenciar centralmente a segurança de dispositivos móveis. No próximo capítulo serão apresentados os trabalhos relacionados à temática desta dissertação.

3 TRABALHOS RELACIONADOS

Neste capítulo, serão apresentados os principais trabalhos que se relacionam de alguma forma com a temática desta dissertação.

3.1 DESCRIÇÃO DAS INICIATIVAS

O primeiro trabalho relacionado a ser destacado neste capítulo é [Jeter 2013], cuja ideia principal consiste em apresentar uma análise dos dados de questionários sobre o comportamento do usuário relacionado à segurança na utilização do dispositivo móvel *Android*. Alguns dados analisados são: se o *Bluetooth* está ativado, se o usuário fez *root* no dispositivo móvel, se recursos de acessibilidade de necessidades físicas estão ativados, se a localização GPS está ativada, dentre outros.

Com base nos dados recolhidos, a iniciativa identifica as mais significativas ameaças aos usuários, e possíveis soluções são apresentadas/recomendadas. Adicionalmente, através de um aplicativo específico, o trabalho testa o conhecimento de segurança do usuário através de perguntas sobre as funcionalidades do *smartphone*; esta funcionalidade se encontra na aplicação chamada de "*Test Your Phone*", e tem o intuito de verificar possíveis falhas de segurança provenientes da falta de conhecimento técnico do usuário final. Essas falhas são divididas em seis categorias: senhas, mensagens de texto e chamadas, aplicações, recursos básicos do *Android*, permissões e *root*.

Um ponto de destaque desse trabalho é mostrar para o usuário possíveis problemas de segurança relacionados à configuração do *smartphone*, deixando o dispositivo móvel menos vulnerável a ataques. Apesar disto, o trabalho não avalia efetivamente o *smartphone* e nem o configura, o que seria um ponto importante, pois nem sempre o que o usuário responde nas perguntas está efetivamente implementado no dispositivo móvel.

Em outro trabalho relacionado relevante, Braga [Braga 2012] apresenta um estudo de caso referente ao tratamento das ameaças e vulnerabilidades relacionadas às plataformas modernas de dispositivos móveis. No estudo realizado em vários dispositivos móveis foi visto que uma das principais causas de ameaças e vulnerabilidades está relacionada à má configuração do usuário. Principalmente no que se diz a respeito ao controle de acesso ao dispositivo móvel, o estudo de caso mostra que o usuário deve ter um tipo senha definido para que o acesso ao sistema possa ser mais seguro, e no caso o *Android* conta com modos com diferentes níveis de segurança para bloqueio da tela inicial: 1- Reconhecimento Facial, 2- Padrão de desenho, 3- Senha e 4- PIN (*Personal Identification Number*).

Outro ponto do estudo de caso é em relação às Restrições de Acesso ao dispositivo móvel, no qual explica que fazer o *rooting* do dispositivo móvel pode o deixar vulnerável, pelo fato de o sistema impossibilitar que o usuário instale aplicativos com permissões de superusuário, o que concederia tais permissões ao aplicativo em questão [Play 2016].

Uma lacuna importante deste trabalho é a falta de itens relacionados focados especificamente na segurança das conexões, que é um item relevante quando se trata de segurança de dispositivos móveis.

Em outra iniciativa relevante, Zefferer [Zefferer 2013] desenvolveu uma API para a análise do comportamento do dispositivo móvel através de uma avaliação de 22 propriedades de segurança pré-definidas. Algumas propriedades se destacam neste contexto, em especial: I) para acessar o *smartphone*, o usuário deve configurar uma senha contendo caracteres e numéricos, II) verificar se a criptografia foi ativada, III) verificar se nenhum teclado alternativo está instalado, IV) verificar se nenhum aplicativo suspeito foi registrado para receber mensagens SMS no dispositivo, dentre outros. Um ponto negativo deste trabalho é que API só funciona via Web, ou seja, é preciso o usuário estar conectado a *Internet* para fazer a checagem no dispositivo móvel. Outra restrição é a limitação de propriedades, pois poderiam também ser abordadas propriedades como: *Bluetooth* ativado, ancoragem com

senha, aplicações suspeitas com acesso ao GPS, entre outras, que podem deixar o dispositivo móvel menos vulnerável a outras situações ou formas de ataques.

Em outra iniciativa importante Vecchiato [Vecchiato 2015], os autores desenvolveram uma aplicação chamada “Avaliação de Segurança”, que tem por objetivo auxiliar o usuário a verificar as configurações do dispositivo móvel em diferentes níveis de segurança. A aplicação basicamente avalia a segurança de dispositivos *Android* com base nas configurações definidas pelos usuários.

Esta aplicação extrai 14 níveis de segurança automaticamente, e esses níveis são baseados nas configurações dos usuários dos dispositivos móveis. As informações sobre essas configurações são enviadas para um serviço Web externo, o qual contém uma lista pré-definida de segurança de cada nível para fazer uma comparação dos níveis colhidos no dispositivo móvel com uma lista. Por exemplo, na lista contida no serviço web, o nível “antivírus” contém um banco de dados com as seguintes informações: duas listas de *malwares,* a primeira foi extraída do projeto *Malgenome* [ZhouY 2012] que fornece uma grande coleção de 1.260 *malware*s em *Android* e a outra lista criada com base em uma pesquisa aprofundada para aplicações de segurança no *Google Play* e vários fóruns para desenvolvedores, por exemplo [xdadevelopers 2016] e [stackoverow 2016]; depois de extrair os dados retorna do serviço Web uma resposta para o usuário, e essa resposta contém o “resultado” que mostra quais níveis precisam ser consertados e “como consertar”. Os principais níveis propostos na aplicação são: Redes (que verifica problemas de rede como, por exemplo, se alguma criptografia é utilizada), Localização (verificar se GPS está ligado), Fontes Desconhecidas (utilização de aplicativos não oficiais da loja do *Google Play*) e Antivírus (verificar possíveis *malwares* no dispositivo móvel).

A aplicação proposta ajuda o usuário a ter uma configuração mais segura e se prevenir dos riscos de uma má configuração, porém ela poderia focar em outras configurações mais específicas como: verificar criptografia do cartão de memória, verificar se o *Bluetooth* está ligado, verificar aplicativos que

consumem muita bateria e verificar aplicativos que sobrecarregam o dispositivo em termos de processamento. Adicionalmente, no nível “Localização”, a aplicação apenas verifica se GPS está ligado; no entanto, seria também importante verificar se existem aplicativos que utilizam o GPS sem permissão.

3.2 DISCUSSÃO COMPARATIVA

Diante dos trabalhos apresentados, pode-se afirmar que [Jeter 2013] e [Braga 2012] focaram na análise do comportamento do usuário, um dos pontos é aplicativo *Test Your Phone,* que apenas testa o conhecimento de segurança através de perguntas sobre as funcionalidades do *smartphone,* e sabe-se que nem sempre o que usuário responde condiz na prática.

Outro ponto importante é que faltou uma abordagem em aplicativos relevantes e necessário para a má configuração do usuário como, por exemplo, verificar criptografia do cartão de memória, verificar se o está ligado, verificar aplicativos que consumem muita bateria e verificar aplicativos que sobrecarregam o dispositivo em termos de processamento.

Por outro lado, outras iniciativas apresentadas [Zefferer 2013] e [Vecchiato 2015] propuseram a checagem, em tempo real, do dispositivo móvel do usuário, em busca de possíveis brechas de segurança oriundos da má-configuração por parte deste usuário. Esta abordagem se mostrou mais interessante, pois nem sempre o fato do usuário ter o conhecimento de segurança implica que ele fará uma configuração menos arriscada do dispositivo (esse fato inclusive será mostrado no capítulo de avaliação deste trabalho).

Contudo, essas iniciativas focaram em problemas de segurança específicos, e não se basearam explicitamente em nenhuma das cartilhas referências importantes explicados no Capítulo 2; por isso, pontos importantes como: *Bluetooth* está ligado, verificar aplicativos que consumem muita bateria, verificar aplicativos que sobrecarregam o dispositivo em termos de

processamento, ancoragem com senha, aplicações suspeitas com acesso ao GPS e outros relacionados à má configuração do usuário acabaram não sendo abordados nessas iniciativas.

3.3 CONSIDERAÇÕES FINAIS

Nesta seção foram apresentados os principais trabalhos relacionados à temática proposta nesta dissertação, e após a análise dos mesmos foi possível verificar que existe uma lacuna referente a uma solução voltada para a avaliação de má configuração do usuário e que seja baseada em cartilhas ou referências de segurança amplamente adotadas (como as explicadas no Capítulo 2).

Ainda foi mostrada uma discussão comparativa destas iniciativas. No próximo capítulo, será apresentada a solução MSC, a qual foi proposta observando a possibilidade de preencher esta lacuna identificada.

4 MOBILE SECURITY CHECK: UMA SOLUÇÃO PARA A MELHORIA DA SEGURANÇA DE DISPOSITIVOS MÓVEIS *ANDROID*

O objetivo geral deste trabalho é desenvolver uma solução que possa mitigar problemas de segurança advindos de más configurações por parte dos usuários em dispositivos móveis. Em outras palavras, uma estratégia que possa checar, informar e classificar possíveis configurações nos dispositivos móveis por parte do usuário que tragam riscos de segurança ao dispositivo e aos dados sensíveis nele armazenados.

A base de segurança associada a este trabalho foi elaborada através de pesquisas de artigos e cartilhas de segurança da NIST [Souppaya *et al* 2013] e do CERT [CERT.br 2013], Ambas já comentadas no Capítulo 2. Esta solução foi implementada baseada no sistema operacional *Android,* por ser o mais utilizado e o mais visado por pessoas mal intencionadas [Storn 2014] e está atualmente disponível na loja virtual associada a este sistema operacional. A estruturação deste capítulo está dividida da seguinte forma. A Seção 4.1 aborda os Requisitos da Solução MSC. Na Seção 4.2, é detalhada a Arquitetura do MSC, na seção 4.3 mostra a Visão geral da solução e na seção 4.4 A implementação e na seção 4.5 considerações finais.

4.1 REQUISITOS

Nesta seção, serão detalhados os requisitos funcionais e não funcionais considerados para o desenvolvimento da solução proposta. Em especial, os requisitos funcionais foram extraídas das referências relevantes dentro da temática, em especial a cartilha de segurança do [CERT.br 2013], a cartilha da [CAIS/RNP 2012], do minicurso de Segurança da Informação e de Sistemas Computacionais do XII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG) [Braga 2012] e do guia de recomendações do NIST [Souppaya and Scarfone 2013]. Com isso, foi

elaborado um estudo comparativo com os itens funcionais mais importantes de segurança em dispositivos móveis que serão descritos na Tabela 4.1.

Tabela 4.1- Estudo comparativo dos itens presentes nas referências básicas

Itens Funcionais	Cartilha do CERT	Cartilha do CAIS	SBSEG	NIST
1. Arquivos SMS (Serviço de Mensagens Curtas) armazenadas no dispositivo móvel	X	X	X	
2. Cuidados ao usar redes WI-FI públicas	X	X	X	X
3. Realizar o *Jailbreak* ou *Root*	X		X	
4. Utilizar um antivírus	X	X		
5. *Bluetooth* desabilitado	X			X
6. Instalar aplicativos de fontes não seguras	X	X	X	X
7. Evitar aplicativos suspeitos que utilizam o GPS	X	X		X
8. Manter as informações sensíveis sempre em formato criptografado	X	X	X	X
9. Bloqueio de tela	X	X	X	X
10. Aplicativos com alto consumo do plano de dados		X	X	
11. Aplicativos que demandam muito processamento		X	X	
12. Aplicativos com alto consumo de bateria		X	X	
13. Existência de conexão P2P	X			
14. Ancoragem com senha	X		X	
15. Qualidade da senha da ancoragem	X		X	
16. Segurança dos dados trafegados	X	X		X
17. Existência de aplicativos suspeitos com acesso à Agenda	X	X		
18. Perda do dispositivo móvel	X		X	
19. Verificar as assinaturas digitais em aplicativos				X

O estudo comparativo mostra que os itens 1-“Arquivos SMS (Serviço de Mensagens Curtas) armazenados no dispositivo móvel”, 2- “Cuidados ao usar redes WI-FI públicas”, 6- “Instalar aplicativos de fonte não segura”, 8- “Manter as informações sensíveis sempre em formato criptografado” e 9- “Bloqueio de tela”, no comparativo dos itens funcionais foi os que estavam presentes em todas as referências, pelo fato de serem os mais deixam vulneráveis na questão da má configuração do dispositivo móvel por parte do usuário. Desta forma, eles estão automaticamente inseridos dentro dos requisitos funcionais da solução que serão explicitados na próxima subseção, a 4.1.1.

Outros itens como: 4- Utilizar um antivírus, 5- *Bluetooth* desabilitado, 6- Instalar aplicativos de fontes não seguras, 7-Evitar aplicativos suspeitos que utilizam o GPS e 8- Manter as informações sensíveis sempre em formato criptografado.

4.1.1 Requisitos Funcionais

Nesta subseção serão detalhados os requisitos funcionais considerados para o desenvolvimento da solução proposta.

[RF 01] Verificar se a senha de bloqueio de tela do aparelho está configurada. Em caso de perda ou roubo do dispositivo móvel, o uso de senha de bloqueio dificultará a violação dos dados armazenados no dispositivo móvel. Além disto, é importante verificar se há utilização de uma senha com números e/ou letras, pois o método deslizar o dedo não é considerado seguro, visto que, colocando-se o dispositivo móvel contra a luz qualquer pessoa pode ver o contorno por onde foi feito o deslize.

[RF 02] Efetuar busca por aplicativos instalados obtidos em locais não oficiais. Instalar aplicativos de fontes confiáveis, como lojas oficiais, diminui a possibilidade vírus ou código malicioso.

[RF 03] Verificar se o cartão de memória está criptografado. A importância desta verificação se deve ao fato de que o cartão de memória sem criptografia deixa os dados sensíveis sujeitos a maior chance de violações por pessoas mal intencionadas.

[RF 04] Checar se há aplicações com acesso a leitura dos SMS. Todo aplicativo instalado pede permissão para acessar diversos recursos do dispositivo móvel, por isso é importante certificar das reais permissões que o aplicativo necessita. Em especial, um aplicativo malicioso com acesso a leitura do SMS do usuário poderá tirar vantagem desse acesso para fazer ataques ou enviar mensagens sem a permissão do usuário.

[RF 05] Verificar se o usuário ativou a ancoragem/roteamento de Internet utilizando senha. É comum os usuários configurarem o dispositivo móvel como um roteador para compartilhamento da *Internet*. Contudo**,** rotear o sinal do WI-FI sem senha deixa o dispositivo móvel vulnerável a ataques por pessoas mal intencionadas.

[RF 06] Verificar se a senha usada para a ancoragem da *Internet* é fraca. O uso de uma senha fraca é quando não se tem a combinação de letras, números e caracteres, sendo fundamental evitar o seu uso para dificultar o acesso ao dispositivo móvel por pessoas mal intencionadas.

[RF 07] Procurar por aplicações que tem acesso ao recurso de GPS. Existem aplicativos maliciosos que solicitam permissão de acesso ao GPS sem mesmo precisar, sendo um risco para o usuário, pois uma pessoa mal intencionada poderá ativá-lo e a localização do usuário pode ser enviada a um destinatário desconhecido.

[RF 08] Verificar se existe o uso de conexão P2P. Neste tipo de conexão, é difícil saber a origem do arquivo que está se baixando. Além disso, é também difícil atestar se um arquivo é ou não seguro.

[RF 09] Verificar se existem aplicativos com acesso à Agenda do dispositivo móvel. Em tese, apenas aplicativos de mensagens de texto, redes sociais e agendas de contatos utilizam a agenda do dispositivo. É importante alertar ao usuário que outras aplicações também fazem uso da mesma.

[RF 10] Verificar se a conexão via Bluetooth está ativada. O *Bluetooth* ativo deixa o dispositivo móvel vulnerável a ataques ou roubo de informações pela conexão sem fio. Além disso, o *Bluetooth* ativo ocasiona desnecessariamente consumo de energia que poderia ser evitado, degradando a carga de bateria do dispositivo móvel.

[RF 11] Verificar se a Conexão WI-FI está usando algum mecanismo de segurança. Utilizar a conexão com criptografia deixa os dados sensíveis menos suscetíveis a ataques pela rede, especialmente interceptação e adulteração.

[RF 12] Procurar aplicativos suspeitos (maliciosos). Aplicativos com códigos maliciosos ou mal intencionados podem fazer vários tipos de ataques aos dispositivos móveis dos usuários, principalmente o ataque homem no meio [Grossmann 2014], no qual a pessoa mal intencionada fica no meio da conexão do usuário com a *Internet* e assim pode interceptar os dados da conexão, e esses dados trocados entre duas partes podem ser manipulados.

[RF 13] A solução deve verificar se o usuário utiliza um antivírus recomendado. A utilização de antivírus é tradicionalmente sugerida na computação. Neste caso, a solução deve verificar se um antivírus “recomendado” está sendo usado; caso contrário, a solução sugere o uso de 11 antivírus com melhores pontuações em usabilidade, performance e proteção e que são direcionados para dispositivos móveis *Android*, de acordo com o estudo da [AV-TEST, 2016]. Alguns critérios que são avaliados para a escolha dos 11 melhores antivírus são: “A detecção do *malware* mais recente *Android* descoberto nas últimas 4 semanas”, na parte de proteção. Em desempenho os critérios foram: Desempenho: “O aplicativo não afeta a vida da bateria”, “O aplicativo não abrandar o dispositivo durante o uso normal”, “O aplicativo não gera muito tráfego” e entre outros. Em usabilidade critério adotado foram “bloquear chamadas de números específicos ou desconhecidos”, Proteção de sites maliciosos e / ou contra *phishing.* Localizar, bloquear ou apagar o seu dispositivo quando ele for perdido ou roubado e entre outros.

[**RF 14] A solução deve procurar e destacar aplicativos que mais consomem o plano de dados.** Muitas vezes alguns aplicativos consomem mais do que o esperado, inclusive não sendo usado pelo usuário frequentemente, e o plano de dados do usuário pode ser esgotado, levando a indisponibilidade da conexão.

[RF 15] Buscar e evidenciar os aplicativos que mais sobrecarregam o processador do dispositivo móvel. Sobrecarregar o sistema como um todo torna o dispositivo mais lento, muitas vezes levando até a indisponibilidade momentânea ou duradoura. É importante que o usuário tenha conhecimento das aplicações instalados no dispositivo móvel que contribuem para este contexto.

[RF 16] Procurar por aplicativos que apresentem alto consumo de energia. Aplicações que se enquadram neste aspecto, além de diminuírem a vida útil da bateria, acabam por ocasionar a indisponibilidade do dispositivo móvel mais rapidamente.

4.1.2 Requisitos não Funcionais

Nesta subseção serão detalhados os requisitos não funcionais considerados para o desenvolvimento da solução proposta.

[RNF 01] A solução deve buscar prover segurança para os dados trafegados. Por ser inclusive uma aplicação de segurança, é desejado que a solução proposta se comunique de forma segura quando precisar enviar dados do usuário por redes inseguras (ex.: Internet) e faz requisições no ambiente externo.

4.2 VISÃO GERAL DA SOLUÇÃO

Com base nos requisitos funcionais e não funcionais descritos na seção anterior foi desenvolvida uma solução denominada *Mobile Security Check* (MSC) para que os dispositivos móveis tenham configurações/decisões

mais segura em relação a segurança em dispositivos móveis. Nesta seção, será apresentada a visão geral da solução. Mais especificamente, a Figura 4.1 mostra os principais componentes desta solução e os passos necessários para a execução da mesma.

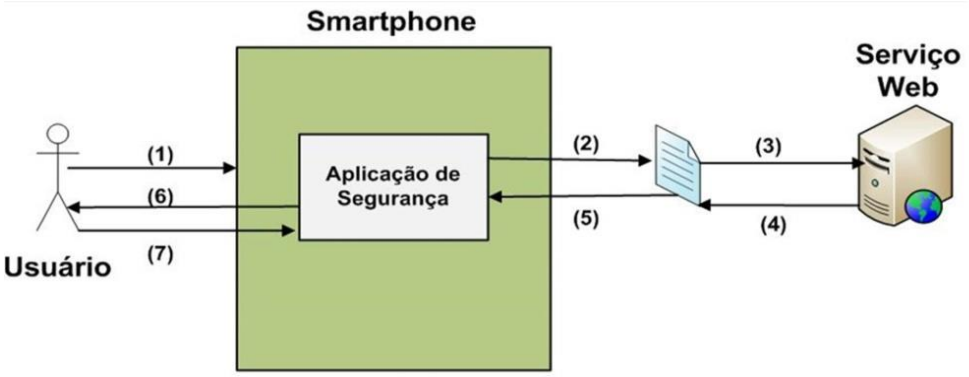


Figura 4.1- Visão geral da solução proposta

Do ponto de vista geral, a solução é instalada no *smartphone* do usuário e se comunica via *Internet* com um serviço Web para obtenção de informações externas de segurança.

A ideia principal é que apenas o item de segurança “Aplicativos maliciosos e/ou suspeitos” utilize a *Internet* para acessar o serviço Web, para que o usuário não dependa somente dela para realizar a checagem por más configurações do dispositivo e também para não sobrecarregar o dispositivo móvel com o sincronismo com o serviço Web, por isso os demais buscam as informações internamente no dispositivo móvel, e não havendo conexão com a internet no momento da checagem, o MSC adiará a verificação do item que necessita do serviço Web e depois o usuário terá que fazer novamente a checagem no dispositivo móvel.

A partir deste momento, serão apresentados os passos necessários à execução da solução proposta neste trabalho e que estão ilustrados na Figura 4.1.

1**. Usuário inicializa a aplicação.** Neste passo, o usuário interage diretamente com a solução MSC e inicia a checagem da segurança.

2**. A solução MSC faz avaliação do dispositivo móvel do usuário.** Neste passo, a checagem é feita internamente em busca de possíveis más configurações do usuário com base em 16 itens pré-definidos, que estão diretamente ligados aos requisitos apresentados na Seção 4.1.

A seguir será apresentado e descrito resumidamente cada um desses 16 itens na Tabela 4.2.

Tabela 4.2- Os 16 itens da solução MSC

	Itens	**Descrição**
I	Senha na tela inicial	Verificar se o usuário configurou uma senha na tela Inicial.
II	Criptografia do Cartão de Memória	Verificar se o cartão de memória está criptografado.
III	Existência de aplicações com acesso à leitura dos SMS	Listar aplicativos que têm acesso à leitura dos SMS.
IV	Ancoragem com senha	Mostrar se usuário configurou uma senha na ancoragem (Roteador WI-FI).
V	Qualidade da senha da ancoragem	Informar ao usuário se a senha da Ancoragem é fraca.
VI	Aplicativos com acesso ao GPS	Listar aplicativos com permissão ao recurso de GPS do dispositivo.
VII	Existência de conexão P2P	Mostrar se o dispositivo está usando conexões P2P (*Peer to Peer*).
VIII	Aplicativos com acesso à Agenda	Listar aplicativos com acesso a agenda do dispositivo móvel.
IX	*Bluetooth* ativo	Informar ao usuário se o *Bluetooth* está ativo.
X	Aplicativos instalados de fonte desconhecida	Mostrar ao usuário aplicativos que não são da loja do *Google Play*.
XI	Conexão WI-FI segura	Indicar se na conexão WI-FI está sendo utilizada Criptografia WPA2
XII	Existência de aplicativos suspeitos	Buscar no Serviço Web por aplicativos considerados suspeitos.

XIII	Antivírus recomendado instalado	Sugerir o uso de antivírus mais recomendados, de acordo com o estudo da [AV-TEST 2016], para dispositivos móveis.
XIV	Aplicativos com alto consumo do plano de dados	Mostrar ao usuário quais são os aplicativos que mais consumem o plano de dados disponível no dispositivo.
XV	Aplicativos que demandam muito processamento	Mostrar ao usuário quais são os aplicativos que sobrecarregam o processamento do dispositivo móvel.
XVI	Aplicativos com alto consumo de bateria	Mostrar ao usuário aplicativos que apresentam um alto consumo de bateria.

3- **A solução MSC envia requisição para o Serviço Web.** Neste passo, o serviço Web recebe uma requisição da solução com o objetivo de verificar possíveis aplicativos suspeitos e/ou maliciosos. O envio desta informação é feita de forma segura, utilizando criptografia SSL para a garantia da confidencialidade. Este serviço Web contém uma lista extensa de aplicativos já classificados como maliciosos pelo CERT (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança). Esta lista contém aplicativos já classificados com códigos maliciosos, por exemplo, não validar o certificado SSL (*Secure Socket Layer*) [Grossmann 2014], por prejudicar o desempenho do dispositivo móvel e por roubo de informações e a sua atualização é feita automaticamente pelo CERT a cada trinta dias e manualmente pelo desenvolvedor da solução diariamente. O SSL é um protocolo desenvolvido para elevar a segurança dos dados transmitidos pela *Internet* e sem o SSL o dispositivo móvel pode ficar mais vulnerável ao ataque conhecido como *Man-in-the-middle*, ataque comum para roubar informações [Grossmann 2014].

4- **O serviço Web encaminha a resposta ao dispositivo móvel.** Neste passo, depois de comparar a lista de aplicativos do usuário com a lista de aplicativos maliciosos, o serviço Web encaminha uma resposta listando possíveis aplicativos maliciosos ou a mensagem “Não existem aplicativos suspeitos (maliciosos)”.

5- **O resultado chega ao dispositivo móvel.** Neste passo, a solução, de posse da resposta do serviço Web, faz a integração dos resultados juntamente com o resultado dos 15 itens da checagem interna totalizando os 16 itens. Neste momento, a solução irá verificar o nível de segurança que o dispositivo móvel se encontra (Baixo, Médio ou Alto).

6- **A solução mostra qual a classificação do nível de Segurança em que o dispositivo móvel se encontra e fornece sugestões de melhoria de configuração.** Neste passo, a solução mostra para o usuário em que nível de segurança seu dispositivo móvel se encontra (Baixa, Média ou Alta) e também informa sugestões de como melhorar, eliminar ou mitigar os riscos de segurança encontrados.

Tendo em vista os diversos itens da Tabela 4.2, foi elaborada uma tabela para medir o grau de gravidade relativa à ocorrência do evento para o usuário. Essa gravidade pode ser descrita através da equação gravidade = probabilidade de ocorrência x impacto associado. A probabilidade está relacionada à probabilidade da ocorrência do evento e o impacto associado quantifica a dimensão dos prejuízos advindos da ocorrência do evento. Esta equação foi inspirada no PMBOK (*Project Management Body of Knowledge*) [PMBOK 2014], que sugere técnicas para a valoração de riscos. A Tabela 4.3 ilustra o contexto explicado.

Tabela 4.3 - Quantificação dos itens de Segurança

Categoria:	Itens de Segurança
Probabilidade	(1) Baixa (2) Média (3) Alta
Impacto	(1) Baixa (2) Média (3) Alta
Gravidade	= Probabilidade x Impacto
Se a Gravidade variar de: 1 e 2-Baixo Risco 3 e 4-Médio Risco 6 e 9-Alto Risco	

Os itens funcionais “Tela inicial com senha”, “Há aplicativos com acesso ao GPS”, “Cartão de memória não está criptografado” e “Aplicativos que consomem muito a bateria” tiveram presentes em 3 ou mais referências básicas do estudo comparativo descritos na Tabela 4.1 e também pelo risco causado ao usuário pela má configuração desses itens formaram o nível de gravidade “Alto”.

Os itens funcionais que estiveram presentes em 2 referências e com risco moderado para o usuário pela má configuração formaram o nível “Médio” e os itens “Conexão WI-FI é segura (WPA2)”, “Aplicativos que mais consomem o plano de dados”, “Há aplicações com acesso a leitura dos SMS”, “Não há conexão P2P (Peer to Peer)” e “Há Aplicativos com acesso à Agenda” presentes em 2 referências, mas com riso baixo para o usuário e que não são relacionados a má configuração do usuário formam os itens de gravidade “Baixo”. Conforme mostra a tabela 4.4 para a distribuição dos itens de segurança com seu respectivo nível de gravidade.

Tabela 4.4- Itens de segurança com seu respectivo nível de gravidade

Itens de segurança	Nível de Gravidade
Tela inicial com senha	Alto
Há aplicativos com acesso ao GPS	Alto
Cartão de memória não está criptografado	Alto
Aplicativos que consomem muito a bateria	Alto
Você não tem um antivírus recomendado instalado	Médio
Bluetooth está ativado	Médio
Sua ancoragem (Rotear o WI-FI) tem senha	Médio
Sua ancoragem (Rotear o WI-FI) tem senha fraca	Médio

Existem aplicativos suspeitos (Maliciosos)	Médio
Aplicativos instalados de fonte desconhecida	Médio
Aplicativos que sobrecarregam o sistema do *Android*	Médio
Conexão WI-FI é segura (WPA2)	Baixo
Aplicativos que mais consomem o plano de dados	Baixo
Há aplicações com acesso a leitura dos SMS	Baixo
Não há conexão P2P (*Peer to Peer*)	Baixo
Há Aplicativos com acesso à Agenda	Baixo

7- **O usuário interage com o dispositivo móvel.** Neste passo, o usuário clica em cima de cada item do dispositivo móvel que mostrará um alerta para o usuário com dicas e como corrigir eventuais falhas de segurança.

A avaliação final da classificação do nível de Segurança do dispositivo móvel pode ser Baixa, Média ou Alta seguindo as seguintes considerações:

1- Em relação à má configuração do usuário, o dispositivo móvel que tiver o resultado de dois itens de segurança do nível baixo marcado com o “X” conforme mostra a figura 4.3, o dispositivo móvel será classificado como alto nível de segurança;
2- Não havendo itens de segurança marcados com “X” na classificação do nível Baixo, mas havendo dois itens de segurança Médio marcados, o dispositivo móvel será classificado como Médio;
3- Havendo dois ou mais itens de segurança do nível Alto marcados com “X” automaticamente o MSC classificará como nível baixo de segurança.

4.3 ARQUITETURA DO MSC

A arquitetura é a definição dos elementos como classes e componentes e como eles se relacionam dentro da solução MSC. A seguir será destacado as classes da inicialização da tela da solução pelo usuário, a primeira são as classes da checagem no dispositivo móvel, a segunda classe é o acesso ao serviço Web e as classes do nível de segurança do dispositivo móvel.

1- “Iniciar a checagem” utilizada a classe “*MainActivity”.*
2- Após a inicialização tendo como ponto de partida as classes “*orderIncategory”* e “*showAsAction”* responsáveis pela tela de início da solução.
3- As classes new *ProgressesDialog* (v.Getcontext) para exibir a mensagem para o usuário “Carregando” ; “Aguarde um pouco”.
4- Ainda na tela de inicio outras classes importantes para a construção da tela inicial da solução são “ListaVulnerabilidades*Activity.class”*, “ListaSobre.*class* “e “ListaAjuda2.*class*”.
5- Através da classe “mensagem” é enviada uma requisição para o Serviço Web. Mais detalhes na seção 4.2 em Visão geral da Solução.

Uma visão geral do diagrama de classe da solução pode ser visualizada na figura 4.2.

6-

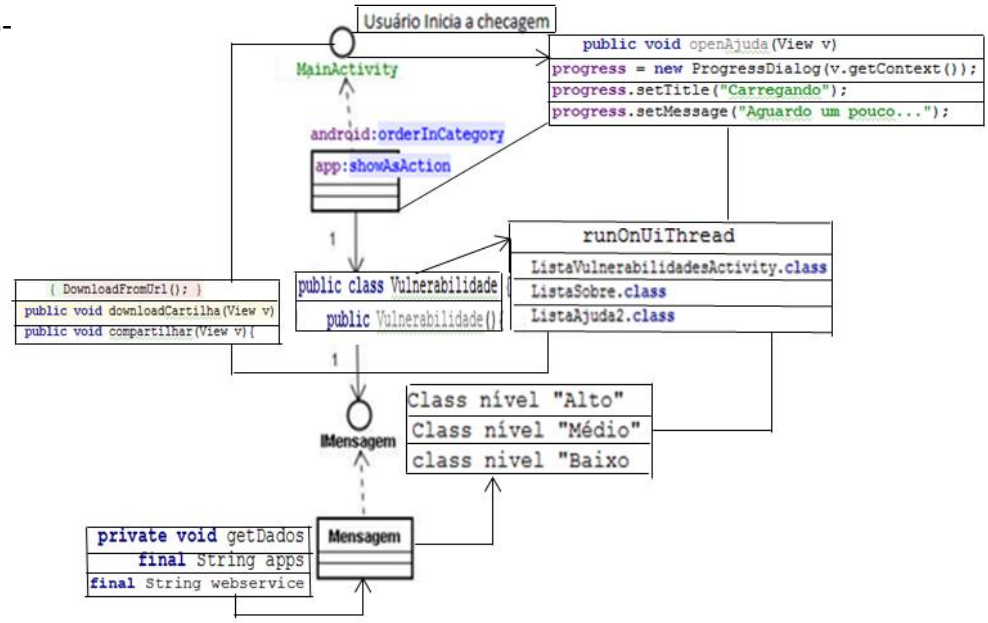


Figura 4. 2- Diagrama de Classe da solução

6- Depois da classe “mesagem” enviar a requisição ao serviço Web a classe getDados faz o comparativo com a lista do serviço Web e caminha a resposta para o usuário utilizando a classe “mensagem”.

Outras classes utilizadas do Android para a checagem dos itens de segurança da solução no dispositivo móvel do usuário serão descritas a seguir:

- A classe SenhaTelaInicial faz uma busca pela classe *lockpatternutils* e utiliza um de seus métodos para verificar se há bloqueio ou não de tela do dispositivo móvel. Caso não encontre a classe “*Class.forName”("com.android.internal.widget.LockPatternUtils***"** ou se der um erro posteriormente significa que a tela de bloqueio não está implementada ou não está funcionando, ou seja, no caso o usuário não configurou uma senha na tela inicial.
- Outra classe “*AppsPermissaoGps(Context context*)” cria uma lista dos aplicativos instalados para cada aplicativo e consulta as permissões dos aplicativos para poder verificar se existe permissão de acesso pelo código *coarse* (via posicionamento aproximado por transmissão de satélites) ou fine (GPS). Para verificar se a senha está configurada no dispositivo móvel foi utilizado a classe “*access point*”.
- A classe “*apmanage*r” verifica se a senha tem menos de 6 dígitos ou se tem os caracteres necessários para a construção de uma senha forte.

4.4 IMPLEMENTAÇÃO

Para a criação da solução MSC foram utilizados a ferramenta gratuita *Android* Studio 2.0 [Studio 2016] e o JDK 7 (Kit de desenvolvimento Java 7) [Oracle 2016]. O MSC oferece suporte para os dispositivos móveis *Android* com as versões 4.0 até a 6.0.

Em termos de interface com o usuário, a solução MSC é composta basicamente por 4 telas. A tela principal possui as seguintes funcionalidades: iniciar a checagem de segurança do dispositivo, disponibilizar informações gerais da solução através dos itens “Ajuda” e “Sobre o Aplicativo”, compartilhar a solução e por fim apresentar a cartilha de segurança do CERT para que o usuário possa esclarecer dúvidas.

Na segunda tela do MSC, são detalhadas as informações referentes aos itens “Ajuda”, o qual explica como utilizar a solução. Por sua vez, a terceira tela apresenta as informações relativas ao item “Sobre o aplicativo”, o qual descreve as características da solução. Por fim, na quarta tela estão dispostos todos os 16 itens relacionados à má configuração do usuário e a classificação do nível de segurança em que o dispositivo móvel do usuário se encontra, conforme mostra a Figura 4.3.

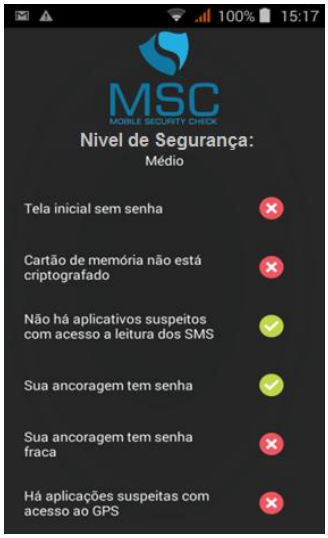


Figura 4. 3- Classificação do nível de segurança

O usuário pode selecionar algum dos itens, e a solução MSC é capaz de prover informações relativas a este item. Por exemplo, no caso da relação do item "Existem aplicações suspeitas com acesso ao GPS", o MSC apresenta a resposta ilustrada na Figura 4.4.

Figura 4.4- Tela do MSC mostrando aplicativos com permissão ao GPS

Alguns dos itens de segurança como: Tela inicial com senha, Cartão de memória não está criptografado, *Bluetooth* não está ativado, Sua ancoragem (Rotear o WI-FI) tem senha e Sua ancoragem (Rotear o WI-FI) tem senha fraca foram implementados usando recursos e informações disponíveis no próprio *smartphone* do usuário. Uma decisão importante foi mostrar que o MSC pode também buscar informação numa lista de aplicativos maliciosos fora da aplicação, utilizando um serviço Web seguro e com isso deixando a aplicação mais dinâmica, pois basta atualizar a lista de aplicativos inseguros no serviço Web, evitando que seja necessária a atualização da versão do aplicativo em si. Como exemplo de item checado usando apenas recursos do dispositivo do usuário, pode-se citar a verificação do tipo de autenticação para rede sem fio (WI-FI) que está sendo utilizada. Exemplos de possíveis conexões são: WEP (*Wired Equivalent Privacy*), WPA (*WI-FI Protected Access*) e WPA2 (*WI-FI Protected Access II*) [Dermatine 2013], e elas podem ser verificadas internamente através do código abaixo.

`fc.controller().getBaixo().WifiSecurityLevel(this)` a variável `WifiSecurity` recebe o valor do método `WifiSecurityLevel` que tem a função de mostrar qual tipo de conexão o dispositivo móvel apresenta.

```
(1) int WifiSecurity =
fc.controller().getBaixo().WifiSecurityLevel(this);
```

```
        String conexao = "";
        switch (WifiSecurity) {
            case (3): {
                conexao = "WPA2";
                break;
            }
            case (2): {
                conexao = "WPA";
                break;
            }
            case (1): {
                conexao = "WEP";
                break;
            }
            case (0): {
      conexao = "Aberto";
                break;
            }
          }
```

O acesso ao serviço Web funciona da seguinte forma: primeiramente, é iniciada a checagem no dispositivo móvel em busca dos aplicativos instalados; após esta atividade, a lista de aplicativos é enviada para o serviço Web com o intuito de fazer a comparação dos aplicativos instalados com a lista de aplicativos maliciosos e assim retorna uma mensagem ao dispositivo móvel caso tenha ou não aplicativo malicioso, conforme mostra o código (2).

```
      private void getDados(){
              final              String              apps              =
fc.controller().getAlto().Apps(ListaVulnerabilidadesActivity.this);
      final              String              webservice              =
http://mercuriosi.com/webservice/api/Aplicativos
              new Thread() {
                  public void run()
                      try {
                       String pg = "package="+apps;
                       String Url = webservice;
                      final String retorno = Util.getData(pg, Url);
```

Finalmente, alguns dos itens da Tabela 4.2 serão descritos neste momento. No caso do item “Você não tem um antivírus recomendado instalado”, ele funciona da seguinte forma: dentro da aplicação existe uma lista dos 11 melhores antivírus com base na avaliação da empresa AV-TEST [AV-TEST 2016], que testa os antivírus considerando a sua usabilidade e proteção. Caso o antivírus do usuário não esteja dentre esses recomendados, o usuário é notificado sobre o fato para proceder com possível mudança.

Nos itens “Aplicativos que sobrecarregam o sistema do *Android*”, “Aplicativos que mais consomem o plano de dados” e para “Aplicativos que consomem muito a bateria” foram criadas duas classificações:

I- Aplicativos com alto consumo de bateria são analisados com base na informação do próprio Sistema Operacional *Android* e acrescido de uma lista pré-determinada que o MSC dispõe que foram tiradas do site *Android pit* [Serowy 2015] e assim são mostrados para o usuário os dois resultados.

II- Aplicativos que sobrecarregam o sistema do *Android* e que mais consomem o plano de dados são analisados por uma lista pré-determinada que a solução MSC dispõe. Em relação ao item II, às vezes, um usuário pode ter uma aplicação específica que tradicionalmente consuma muito (por exemplo, a rede de dados), mas que por esse usuário não usar muito a aplicação ela acaba não apresentando na prática esse problema. Desta forma, destaca-se que a aplicação tem o potencial de consumir muitos recursos, mas que não necessariamente ela estará fazendo isso neste momento.

O estudo se baseou no relatório da AVG (Antivírus Guard) [Serowy 2016] que, a cada trimestre, prepara um relatório com base em dados recolhidos dos milhões de dispositivos móveis de todo o mundo e publica a sua lista dos aplicativos que mais consomem energia.

4.5 CONSIDERAÇÕES FINAIS

Este capítulo descreveu a contribuição principal deste trabalho, que é uma solução para a melhoria das configurações de segurança que o usuário

faz no seu dispositivo móvel. Esta solução, implementada através de uma aplicação denominada *Mobile Security Check*, contribui para a mitigação problemas de segurança advindos de más configurações por parte dos usuários. No próximo capitulo, serão apresentadas as avaliações que foram realizadas para um melhor entendimento da contribuição da solução proposta nesta dissertação.

5 AVALIAÇÃO

Este capítulo tem por finalidade avaliar a solução proposta neste trabalho. Para isso, foram realizadas quatro avaliações. A primeira avaliação consiste na instalação da solução MSC em dois grupos de usuários e posterior checagem de segurança nos *smartphones*. A segunda busca avaliar qual é o nível de entendimento/interesse em relação a segurança de dispositivos móveis pelos usuários destes *smartphones*. Na terceira avaliação, o objetivo é comparar os dados coletados na primeira e segunda avaliações, com o intuito de verificar se os usuários que possuem entendimento ou interesse por segurança costumam adotar boas políticas de configuração. Por fim, na quarta avaliação busca-se mostrar o nível de consumo de energia da solução MSC no dispositivo móvel, com o intuito de avaliar se o mesmo é energeticamente eficiente; isso é importante porque a própria solução MSC sugere o uso de aplicativos que apresentem grau de consumo energético satisfatórios.

5.1 AVALIAÇÃO DA EXECUÇÃO DA SOLUÇÃO MSC EM SMARTPHONES

Nesta avaliação o objetivo é a instalação e execução da solução MSC nos *smartphones* de dois grupos de usuários, cada um com 25 usuários, de ambos os sexos, com idades entre 15 anos e 60 anos que baixaram a solução MSC pelo *Google Play*. O primeiro grupo foi selecionado por ter conhecimento em TI (Tecnologia da Informação) e o outro grupo de usuários, a priori, não possui conhecimento em TI. Optou-se por separar esses dois diferentes grupos para mostrar que mesmo usuários com conhecimento de TI eventualmente adotam decisões de configuração inseguras. Os grupos baixaram a solução MSC pelo *Google Play*. No caso a solução MSC fez a checagem dos itens pré-definidos de segurança nos *smartphones* desses dois grupos, e constatou que todos tiveram um percentual relativamente alto em relação à má configuração do dispositivo móvel, conforme mostra a Tabela 5.1.

Tabela 5.1- Percentual de má configuração nos *smartphones* avaliados

Itens analisados	Usuários TI	Usuários não TI
Cartão de memória não está criptografado	86%	94,1%
Tela inicial sem senha	72%	86%
Ancoragem (roteador WI-FI) não possui senha	70%	90%
Existência de aplicações com acesso à agenda	92%	82,4%
Existência de aplicativos com acesso ao GPS	85%	70,6%
Ancoragem (roteador WI-FI) tem senha fraca	78%	94%
Existência de aplicações com acesso à leitura dos SMS	81%	70,6%
Não há conexão P2P	96%	94,1%
Bluetooth ativado	8%	17,6%
Existência de aplicações instaladas sem ser da loja oficial do Google Play	84%	76,5%
Conexão WI-FI não é segura (uso de criptografia)	100%	100%
Inexistência de aplicativos suspeitos	96%	94,1%
Inexistência de antivírus recomendado	46,5%	63,50%
Existência de aplicativos com alto consumo de bateria	100%	100%
Existência de aplicativos que sobrecarregam o sistema *Android*	96%	94,2%
Alto consumo de dados móveis	94,5%	94,1%

Através da observação dos resultados apresentados na Tabela 5.1, pode-se compreender com mais precisão a importância da solução proposta neste trabalho, principalmente pelo fato dos usuários, em geral, não configurarem ou não se preocuparem em configurar corretamente o *smartphone*, visto que uma grande porcentagem de ocorrências de riscos foi

verificada em situações críticas. Por exemplo, um número considerável de usuários dos dois grupos não criptografa o cartão de memória. Outro exemplo é que, dos usuários com conhecimento em TI, apenas 28% usam senha na tela inicial e 86% não criptografam o cartão de memória; no caso dos usuários sem conhecimento em TI os dados são mais preocupantes, pois 94% utilizam ancoragem (Rotear o WI-FI) com senha fraca e 86% dos usuários utilizam tela inicial sem senha. Com o uso da solução MSC, é possível que o usuário perceba esses pontos falhos; após visualizar e avaliar possíveis ações/soluções, o usuário pode atuar para a melhoria da configuração da segurança do *smartphone*.

5.2 AVALIAÇÃO DO NÍVEL DE ENTENDIMENTO DOS USUÁRIOS SOBRE SEGURANÇA EM COMPUTAÇÃO MÓVEL

Considerando o mesmo conjunto de usuários que instalaram a solução MSC, foi realizada outra avaliação que abordou questões sobre segurança em dispositivos móveis *Android*. Com este intuito, foi elaborado um questionário com perguntas em relação à segurança em dispositivo móveis e sobre alguns itens das cartilhas de segurança anteriormente apresentadas neste trabalho. O resultado desta consulta está apresentado na Tabela 5. **2**

Tabela 5. 2- Nível de entendimento dos usuários

Perguntas	**Respostas dos usuários TI**		**Resposta dos usuários não TI**	
	Sim	**Não**	**Sim**	**Não**
Você tem curso em informática?	44,2%	55,8%	11%	89%
Criptografa o cartão de memória?	38,3%	61,7%	6%	94%
Compartilha a Internet com senha?	76,7%	23,3%	22,5%	77.5%
Bluetooth ativado	18%	82%	73,8%	26,2%
Usa WI-FI com criptografia?	51,2%	48,8%	9%	91%
Possui antivírus?	68,5%	31,5%	36,5%	63,5%

Por sua vez, outro ponto importante é o tipo de bloqueio de tela usado, pois se sabe que o dispositivo móvel sem senha ou com tipo de bloqueio mais simples acaba facilitando o acesso aos dados sensíveis por usuários não autorizados.

Segundo Braga [Braga 2012], o ideal seria utilizar uma senha e um PIN para ter uma maior segurança, porque muitos usuários colocam uma senha fraca. Além disso, o uso do tipo de bloqueio "deslizar" é reconhecidamente inseguro, pois um atacante pode visualizar na tela do dispositivo vestígio sobre qual é o padrão/desenho que sempre é feito pelo usuário. A Figura 5.1 mostra um gráfico com o resultado do questionário relacionado à qual tipo de bloqueio de tela é mais usado pelos usuários com conhecimento em TI.

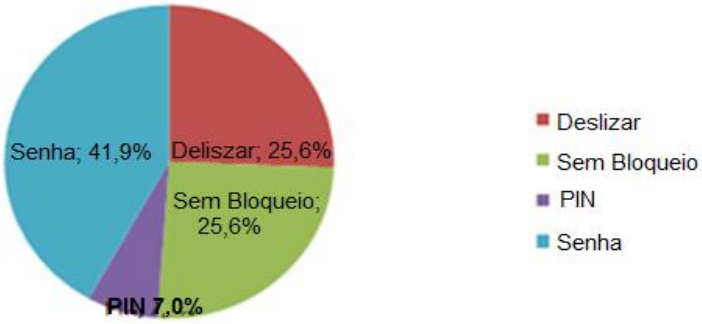


Figura 5.1- Tipo de bloqueio dos usuários TI

Por sua vez, a Figura 5.2 mostra o resultado do questionário relacionado à qual tipo de bloqueio de tela é mais usado pelos usuários sem conhecimento em TI.

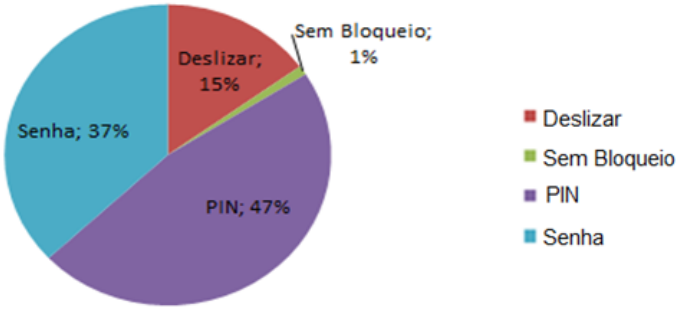


Figura 5.2- Tipo de bloqueio dos usuários sem conhecimento profundo de TI

Os resultados mostram que mesmo com conhecimento em informática e possivelmente dos riscos de segurança pela má configuração dos

dispositivos móveis, muitos usuários não configuram corretamente o *smartphone*. Destacam-se alguns itens da Tabela 5.2, como exemplo o item "*Bluetooth* ativado" com 73,8% para os usuários sem conhecimento em TI, o fato de 61,7% dos usuários com conhecimento em TI não criptografarem o cartão de memória e 91% dos usuários sem conhecimento em TI entrarem na rede WI-FI sem criptografia. Além disso, mais especificamente, a Figura 5.1 mostra que dos quatro tipos de configuração de senha, apenas 41,9% dos usuários de TI colocam senha na tela inicial e a Figura 5.2 mostra que apenas 15% dos usuários "não TI" usam o tipo de bloqueio "senha" na tela inicial; esses números são relevantes e trazem preocupações em relação à segurança dos dispositivos móveis, especialmente considerando a possibilidade de furto do aparelho físico.

5.3 AVALIAÇÃO COMPARATIVA

O principal objetivo da avaliação comparativa é de verificar se, mesmo tendo o conhecimento de segurança, os usuários em geral tomam decisões acertadas em relação às políticas de segurança do aparelho. Para isto, os dados obtidos nas duas avaliações anteriores são cruzados, e os mesmos podem ser vistos na Figura 5.3.

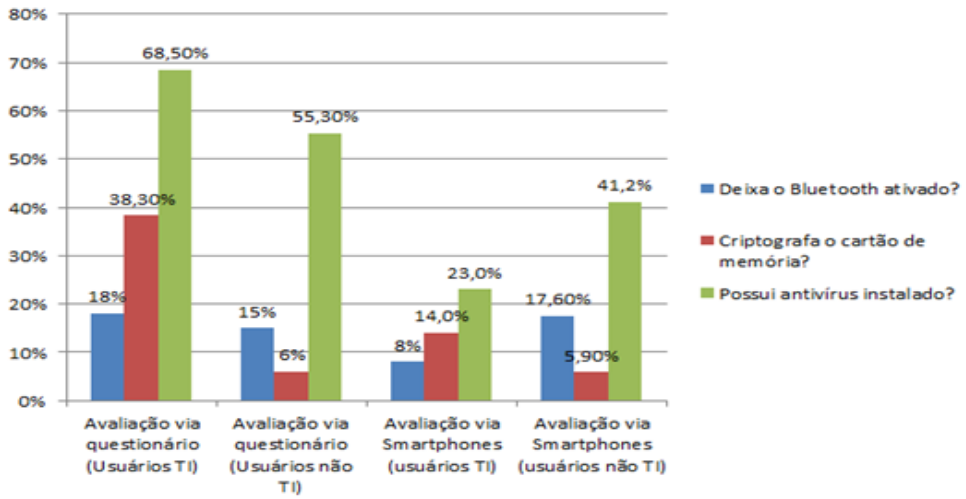


Figura 5.3- Comparativo das avaliações

Este comparativo reforçou ainda mais a necessidade da solução proposta neste trabalho, pois, por exemplo, 38,3% dos usuários com conhecimento em TI afirmam que criptografar o cartão de memória é importante, porém a solução MSC mostrou que apenas 14% o fazem.

Outro dado interessante é que 68,5% desses usuários afirmam que é importante possuir um antivírus instalado e a aplicação mostrou que, na prática, apenas 23% tem um antivírus instalado. No caso dos usuários sem conhecimento de TI, 55,3% afirmam que é necessário possuir um antivírus instalado, porém a solução MSC mostrou que apenas 41,2% possuem um antivírus instalado.

A solução proposta neste trabalho, o MSC, atua diretamente nesta problemática, pois aponta para o usuário quais os problemas que realmente se encontram no *smartphone* naquele momento, e que muitas vezes o usuário esqueceu ou optou por não configurar corretamente, mesmo tendo o conhecimento de que tal configuração pode acarretar em riscos de segurança.

5.4 AVALIAÇÃO DO CONSUMO DE ENERGIA DA SOLUÇÃO MSC

Esta avaliação consiste em mostrar o nível de consumo de energia da solução MSC. A preocupação em fazer essa análise é a de prover uma solução energeticamente eficiente, especialmente quando a mesma aplicação sugere que o usuário utilize apenas aplicações com consumo energético compatível com sua finalidade.

A avaliação se deu da seguinte forma: a solução MSC foi instalada em 10 *smartphones* de marcas diferentes e, para fazer a medição do nível de energia da solução MSC nos *smartphones*, foi instalado o aplicativo *Battery Doctor* [Cheetah 2016]. Este aplicativo é um gerenciador de energia que mede consumo e aumenta a vida útil da bateria, e contém um ranking dos aplicativos com alto consumo de energia de bateria [Mobile, 2016]. Vale ressaltar que mesmo no caso do sistema operacional *Android* ser configurado com a opção

“bateria” (o que depende de sua versão), ainda não é suficiente para fazer uma medição completa de energia de todos os aplicativos instalados, pois esse recurso só avalia os principais aplicativos com alto consumo e recursos do próprio sistema operacional *Android*.

Após iniciar a solução MSC e a deixar em modo *standy-by*, foi visto um aumento do consumo de energia de bateria da solução MSC oscilando entre 2,08% e 2,31%. Após se iniciar a checagem nos *smartphones* dos usuários, o consumo ficou com uma média variando entre 4,87% a 5,03%. Para ser fazer uma avaliação comparativa deste consumo, realizou-se uma busca no aplicativo considerado de "alto consumo" de energia segundo o relatório [AVG 2015], que é um relatório que identifica e mostra consumo de energia de aplicativos em *smartphones Android*. O consumo deste aplicativo, segundo o relatório, é de em média 8%. Considerando que o consumo de energia do MSC está abaixo do aplicativo que menos consome energia dentre os aplicativos tidos como "grande consumidores" de energia, pode-se argumentar que o consumo do MSC está dentro de um padrão de consumo satisfatório.

5.5 CONSIDERAÇÕES FINAIS

O principal objetivo deste capítulo é o de avaliar a solução proposta neste trabalho, o MSC. Para isso, foi realizada a checagem nos *smartphones* de dois grupos de usuários atrás de possíveis configurações inseguras, e a solução foi capaz de detectar essas configurações e alertar a existência das mesmas para os usuários. Adicionalmente, foi visto que mesmo usuários mais experientes em TI também frequentemente adotam políticas inseguras de uso, o que ajuda a reforçar ainda mais a importância da solução proposta. Por fim, a solução ainda apresentou um percentual baixo de consumo de energia da bateria, considerando como comparação o relatório de desempenho de Aplicativos *Android* do AVG (Antivírus Guard) [AVG 2015], que apresenta os aplicativos que mais consomem energia de bateria.

6 CONCLUSÕES E TRABALHOS FUTUROS

Os resultados descritos no presente trabalho mostram que o número de falhas de segurança nas configurações do usuário de dispositivos móveis, em geral, é relativamente alto, e isso leva a uma situação não desejada de insegurança para o mesmo. Tendo isso em vista, este trabalho propôs uma solução para a identificação de configurações inseguras no dispositivo móvel, com o objetivo de minimizar os riscos de segurança associados ao uso do referido dispositivo. Para auxiliar o usuário nesta tarefa, foi desenvolvido o aplicativo MSC (*Mobile Security Check*), que atua para a melhoria das configurações de segurança de dispositivos móveis tendo como base as decisões de configuração do usuário. Implementado na plataforma *Android*, sua função é checar o dispositivo móvel atrás de possíveis más configurações baseada nas principais referências da área de segurança de dispositivos móveis, como o guia de orientações do NIST (National Institute of Standards and Technology) [Souppaya *et al* 2013], a cartilha do CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) [CERT.br 2013] e a cartilha do Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Ensino e Pesquisa [CAIS/RNP 2012]. A solução foi desenvolvida de tal forma que seja possível a incorporação de novas sugestões que forem surgindo nessas ou em outras cartilhas.

6.1 RESULTADOS ALCANÇADOS

No contexto deste trabalho, alguns resultados importantes foram alcançados, e serão brevemente descritos nesta seção.

- Disponibilização de uma solução para a avaliação do nível de segurança do *smartphone*. A solução MSC se encontra disponível para *download* na loja do *Google Play* desde o dia 15 de março de 2016, e até o presente momento possui

aproximadamente 300 downloads de diferentes países. A solução pode ser acessada no seguinte link: https://play.google.com/store/apps/details?id=com.msccheck.check.checker;

- Divulgação do resultado da pesquisa do referencial teórico desta dissertação através de artigo científico em periódico [Cavalcanti, 2015];
- Avaliação do nível de segurança de *smartphones Android* baseada na qualidade das configurações do usuário. Neste trabalho, através dos resultados obtidos na avaliação do mesmo, pode-se inferir que um número expressivo de usuários não configuram corretamente seus *smartphones*, levando o mesmo a um estado de insegurança. Esse fato contribuiu uma maior importância relativa à existência de uma aplicação que possa fazer essa busca por más-configurações e apresenta-las ao usuário;
- Por fim, a implementação da solução foi registrada no NPI (Instituto Nacional de Propriedade Industrial) com o registro de número BR 51 2016 001044 4 com apoio da Universidade Federal Rural de Pernambuco.

6.2 TRABALHOS FUTUROS

Algumas possíveis iniciativas são vislumbradas no contexto futuro deste trabalho. Inicialmente, uma possível melhoria seria o aumento do número dos itens de segurança para checagem da má configuração do usuário. Exemplos de itens importantes incluem, por exemplo, verificar se o usuário deixou as redes sociais ou e-mail conectados; ou seja, sem a necessidade de fazer *login*, tornando o dispositivo um alvo fácil para uma pessoa mal intencionada ter acesso a dados sensíveis.

Outra possibilidade de trabalho futuro é a solução fazer também, em adição as funcionalidades já existentes, a análise estática e dinâmica das aplicações no sistema operacional *Android*:

- Análise estática compreende a verificação do código do *software* em seu estado de texto, antes mesmo dele ser compilado, desta forma possibilitando examinar todos os caminhos de execução possíveis e valores variáveis. A vantagem deste tipo de análise é o melhoramento do nível de segurança, pois é possível verificar o código das aplicações (inclusive usando engenharia reversa, quando só existir disponível o executável da mesma) para analisar esse código e verificar possíveis brechas de segurança.

- A análise dinâmica atua no complemento da estática; ela emula o sistema operacional ou aplicação, e se preocupa com os dados inseridos na rotina, com a saída de dados inseridos (em especial se é a esperada), com o tempo de resposta, com o comportamento funcional e com a performance da aplicação como um todo. A sua principal vantagem é revelar defeitos sutis ou vulnerabilidades cujas origens são muito complexas para serem descobertas na análise estática. A análise dinâmica pode desempenhar um papel importante na tentativa de garantia da segurança, mesmo tendo seu principal objetivo a busca e eliminação de erros (*debug*) [Conviso 2015].

Outro trabalho futuro importante consiste na produção de uma versão em Inglês da solução MSC. Com isto, a mesma poderia ter uma abrangência maior tanto para usuários em si como também para os *feedbacks* da solução em termos mundiais. Em suma, ter a aplicação também em inglês pode facilitar o uso da mesma em outras localidades remotas.

Outra possível iniciativa futura seria a possibilidade da solução poder configurar automaticamente os itens que são checados, se o usuário concordar com as recomendações. De forma prática, o usuário teria duas opções:

configurar os itens desejados individualmente, clicando em cima de cada item, ou clicando no botão “configurar todos os itens”, no qual todos os itens possíveis de configuração automática seriam configurados.

Outra possibilidade de trabalho futuro é fazer uma pesquisa de avaliação da solução MSC nas empresas de tecnologia da informação e profissionais da área de TI para que assim possa ter um retorno para possível melhoria da solução e de outros itens relacionados a má configuração do usuário.

Por fim, planeja-se também o desenvolvimento da solução para outras plataformas, especialmente para *Windows Phone* e IOS. Com a adoção de outras plataformas, naturalmente outros itens de checagem deverão ser avaliados e implementados, possibilitando que a solução seja mais completa e que possa ser usada por um conjunto maior de usuários.

7 REFERÊNCIAS

[Android 2016] S. Android. **Welcome to the Android Open Source Project!.** Disponível em https://source.android.com/. Acesso em 31/08/2016.

[Alliance 2016]*Alliance*. O, *Handset.* Disponível em http://www.openhandsetalliance.com/. Acesso em 30/08/2016.

[AV- TEST 2016]AV- TEST. **The best antivirus software for *Android***. Disponível em https://www.av-test.org/en/antivirus/mobile-devices/. Acesso em 15/04/2016.

[AVG 2015]AVG. **O que é um Malware?** Disponível em http://www.avg.com/a/br-pt/what-is-malware. Acesso em 16/05/2016.

[AVG 2015]AVG. O que é um Spyware? Disponível em http://www.avg.com/a/br-pt/what-is-spyware. Acesso em 17/05/2016.

[Anti-Malware 2016] A, Malwarebytes. Malwarebytes Anti-Malware. Disponível em https://play.google.com/store/apps/details?id=org.malwarebytes.antimalware&hl=pt_BR. Acesso em 20/08/2016.

[Braga 2012] Braga, A. M. , Nascimento, E. N., Palma, L. R. e Rosa, R. P.**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**, SBSeg 2012. Disponível em http://wiki.inf.ufpr.br/maziero/lib/exe/fetch.php?media=ceseg:2012-sbseg-mc2.pdf. Acesso em 19/04/2016.

[CAIS/RNP 2012]CAIS/RNP. **Cartilha de segurança em Dispositivos Móveis**. Disponível em http://www.enq.ufrgs.br/files/Cartilha_de_Seguranca_em_Dispositivos_Moveis.pdf. Acesso em 31/05/2016.

[Canaltech 2014] Canaltech. **Ataques do tipo ransomware a dispositivos móveis são cada vez maiores no Brasil**. Disponível em: http://canaltech.com.br/noticia/seguranca/Ataques-do-tipo-ransomware-a-dispositivos-moveis-sao-cada-vez-maiores-no-Brasil/. Acesso em: 20/04/2016.

[Cavalcanti 2015] Cavalcanti, k., Viana, E. and Lins, F. **Security Issues and Solutions for *Android* -based Mobile Devices**.nternational Journal of Computer Science and Information Security (IJCSIS), Vol. 13, No. 9, September 2015.

[CERT.br 2003] CERT.br. **Práticas de Segurança para Administradores de Redes Internet.** Disponível em http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html. Acesso em 01/09/2016.

[CERT.br 2012] CERT.br. **Segurança em dispositivos móveis**. Disponível em http://cartilha.cert.br/dispositivos-moveis. Acesso em 20//02/2016.

[CIS 2016] CIS, **Center for Internet Security.** Security benchmarks. Disponível em https://benchmarks.cisecurity.org. Acessado em: 22/08/2016.

[check 2016] M, Security Check. **Mobile Security Check**. Disponível em https://play.google.com/store/apps/details?id=com.msccheck.check.checker. Acesso em 30/08/2016.

[Cheetah 2016]Cheetah, M. Inc. **Battery Doctor**. Disponível em https://play.google.com/store/apps/details?id=com.ijinshan.kbatterydoctor_en&hl=pt_BR. Acesso em 06/07/2016.

[Cheetah 2016]Cheetah, M. **Clean Master (Otimizador)**. Disponível em https://play.google.com/store/apps/details?id=com.cleanmaster.mguard. Acesso em 27/07/2016.

[Conviso 2015] Conviso**. Entenda as diferenças entre testes de aplicações dinâmicos e estáticos**. Disponível em http://blog.conviso.com.br/entenda-as-diferencas-entre-testes-de-aplicacoes-dinamicos-e-estaticos/. Acesso em: 15/07/2016.

[D'ARCY 2011]D'arcy, Paul. MARKETING, Large Enterprise. CIO **Strategies for Consumerization: the Future of Enterprise Mobile Computing**. 2011. Disponível em http://www.au-kbc.org/bpmain1/Security/enterprise_mobile_computing.pdf. Acesso em 15/06/2016.

[Dermartine 2013] D. Felipe. **WEP, WPA, WPA2: o que as siglas significam para o seu WiFi?.** Disponível em http://www.tecmundo.com.br/wi-fi/42024-wep-wpa-wpa2-o-que-as-siglas-significam-para-o-seu-wifi-.htm. Acesso em 01/09/2016.

[Dormann 2014] Dormann, W. **Vulnerability Note Database**. Disponível em https://www.kb.cert.org/vuls/id/582497. Acesso em 28/03/2016.

[Grossmann 2015]Grossmann, L.O. **Brasill é o sétimo país no raking global de uso da Internet**. Disponível em http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=39200&sid=4#.VRAQ2fnF98F. Acesso em 10/02/2016.

[Guo 2013]Guo, M. Bhattacharya, P. Yan, M, Qian, K and Yang, L. **Learning mobile security with *Android* security labware**. Proceeding of the 44th ACM technical symposioum on Computer science education March 2013, Pages 675-680.

[IBM 2008]IBM Software Group. **Minimizing code defects to improve software quality and lower development costs**. IBM Rational Software Analyzer and IBM Rational PurifyPlus software. October 2008.

[PMBOK 2014] PMBOK. PMI Standards Committee. A Guide to the Project Management Body Knowledge 2014, PMI Publishing Division, Philadelphia, USA.

[Jeter 2013] Jeter, L., and Shivakant, M. **"Identifying and quantifying the *Android* device users' security risk exposure."** Computing, Networking and Communications (ICNC), 2013 International Conference on 28 Jan. 2013: 11-17.

[Mimoso 2016] Mimoso, Michael. **Scanner Finds Malicious *Android* Apps at Scale**. Disponível em https://threatpost.com/scanner-finds-malicious-*Android* -apps-at-scale/114438/. Acesso em 22/05/2016.

[Mobile 2016] Mobile, AVG. **Antivírus Gratuito para *Android***. Disponível em https://play.google.com/store/apps/details?id=com.antivirus. Acesso em 27/07/2016.

[Novaes 2014] Novaes, Rafael**. Saiba como reconhecer e remover APPs falsos do *Android*** . Disponível em http://www.psafe.com/blog/saiba-como-reconhecer-remover-apps-falsos-*Android* /. Acesso em 20/06/**2016.**

[Oracle 2016] Oracle. **Java SE Development Kit 7 Downloads**. Disponível em http://www.oracle.com/technetwork/pt/java/javase/downloads/jdk7-downloads-1880260.html.html. Acesso em 22/08/2016.

[Overflow 2015]S. Overflow. Stackoverflow. Disponível em stackoverflow.com. Acesso em 21/07/2016.

[Play 2016] P, Google. **Google Play**. Disponível em https://play.google.com/store?hl=pt_BR. Acesso em 20/08/2016

[Player 2016]Flash, **Adobe Player**. Disponível em http://www.adobe.com/br/products/flashplayer.html. Acesso em 20/08/2016.

[Qualcomm 2015]Qualcomm, C. Experiences, **Inc. Snapdragon™ BatteryGuru**. Disponível em https://play.google.com/store/apps/details?id=com.xiam.snapdragon.app&hl=pt_BR. Acesso em 19/07/2016.

[Roberts 2014] Roberts, J. AVG. **AVG *Android* App Performance Report Q4 2014 *Android***. Disponível em http://now.avg.com/avg-*Android* -app-performance-report-q4-2014-presskit/. Acesso em 07/07/2016.

[Romer 2015]R. **Brasil concentra 92% dos casos de ransomware na América Latina**. Disponível em http://corporate.canaltech.com.br/noticia/protecao-de-dados/brasil-concentra-92-dos-casos-de-ransomware-na-america-latina-48259/. Acesso em 16/03/2016.

[Salutes 2016] B. Salutes. **Como fazer backup no Android: diga adeus às perdas de arquivos!**. Disponível em http://www.androidpit.com.br/backup-android. Acesso em 01/09/2016.

[Serowy 2015]Serowy, S. **Aplicativos que mais consomem a bateria e o plano de dados do seu celular**. Disponível em http://www.*Android* pit.com.br/aplicativos-que-mais-consomem-bateria-dados. Acesso em 29/03/2016.

[Souppaya *et al* 2013]Souppaya, M. and Scarfone, K. **Guidelines for Managing the Security of Mobile Devices in the Enterprise**. Disponível em http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf. Acesso em 15/06/2016.

[Soares 2014]Soares, D. **Como Visualizar Aplicativos e Serviços que Gastam Mais Bateria.** Disponível em http://www.escola*Android* .com/como-visualizar-gasto-de-bateria/. Acesso em 05/07/2016.

[Storm 2016]Storm, D. **98% dos *Malwares* tem como alvo a plataforma *Android***. Disponível em http://www.computerworld.com/article/2475964/. Acesso em 19/03/2016.

[Studio 2015]Studio, D. App. **DU Battery Saver.** Disponível em https://play.google.com/store/apps/details?id=com.dianxinos.dxbs&hl=p_BR. Acesso em 19/07/2016.

[Studio 2016] Studio, A. ***Android* Studio.** Disponível em https://developer.*Android* .com/studio/index.html. Acesso em 21/08/2016.

[Vecchiato 2015]Vecchiato, D, Vieira, M and Martins, L. **A security configuration assessment for *Android* devices.** Proceedings of the 30th Annual ACM Symposium on Applied Computing April 2015.

[**Xdadevelopers 2015]** Xdadevelopers. **Forum.xda-developers**. Disponível em forum.xda-developers.com. Acesso em: 21/07/2016.

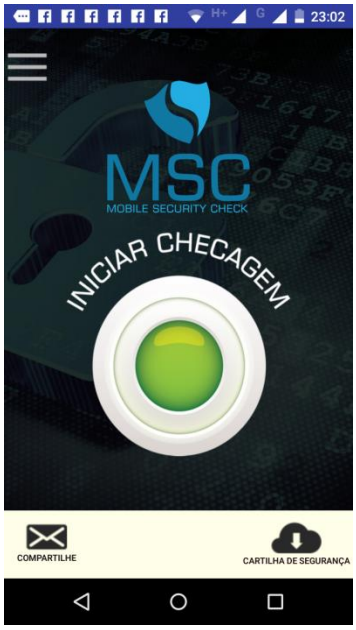
[Zefferer 2013]Zefferer, T. and Teufl , P. **Policy-based Security Assessment of Mobile End-User Devices An Alternative to Mobile**

Device Management Solutions for *Android* Smartphones . Conference on 2013 International, 29-31 July 2013.

[ZhouY 2012]Zhou and X. Jiang.Dissecting *Android* malware: **Characterization and evolution**. In Security and Privacy (SP), 2012 IEEE **[Symposium 2012]** Symposium on, pages 95 -109, May 2012.

APÊNDICE

Apêndice A – Tela inicial da solução MSC.



Apêndice B –Tela onde mostra os menus “Ajuda” e “Sobre o aplicativo”

Apêndice C – Relatório da checagem da solução MSC após a instalação nos *smartphones* dos 25 usuários TI e 25 usuários não TI.

Tela inicial com senha

Cartão de memória não criptografado

Existem aplicativos suspeitos com acesso à leitura dos sms

Sua ancoragem tem senha

Sua ancoragem tem senha fraca

Há aplicações suspeitas com acesso ao GPS

Não há conexão P2P

Há aplicações suspeitas com acesso à agenda

Bluetooth não está ativo

Há aplicações instaladas externamente

Sua conexão WI-FI é segura

Não existem aplicativos suspeitos

Você tem um antivírus recomendado instalado

Alto consumo de bateria

Dispositivo sobrecarregado

Você tem um alto consumo de dados móveis

Apêndice D – Perguntas do questionário da Avaliação de Segurança em *Android* realizada com 25 usuários de TI e 25 usuários não TI.

Você tem curso de informática?

Qual bloqueio de tela usado no *Android*?

Cartão de memória criptografado?

Compartilha internet com senha?

Usa *Bluetooth* com senha?

Usa sempre WI-FI com criptografia?

Possui instalado antivírus?