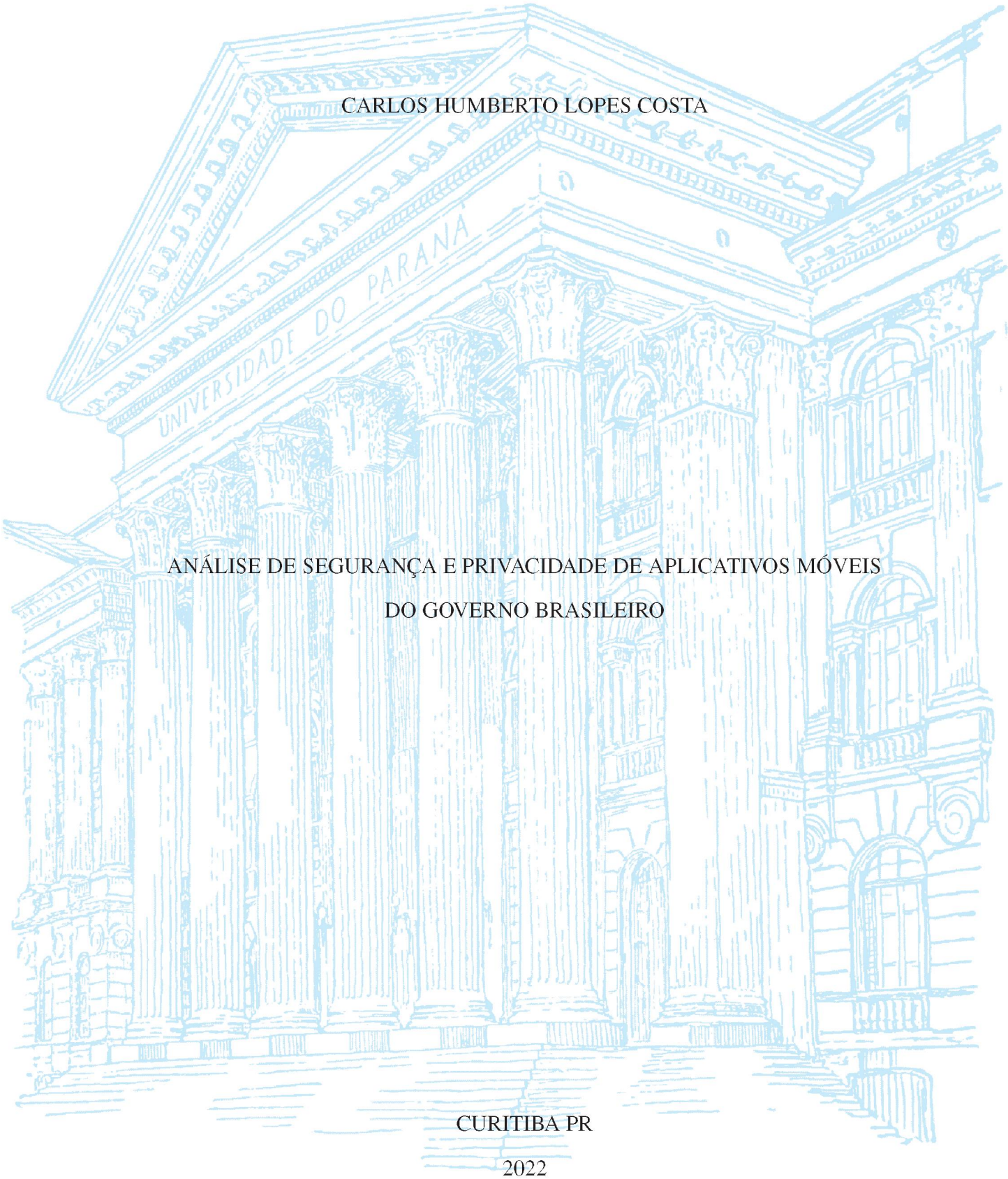
UNIVERSIDADE FEDERAL DO PARANÁ

CARLOS HUMBERTO LOPES COSTA



ANÁLISE DE SEGURANÇA E PRIVACIDADE DE APLICATIVOS MÓVEIS DO GOVERNO BRASILEIRO

CURITIBA PR

2022

CARLOS HUMBERTO LOPES COSTA

ANÁLISE DE SEGURANÇA E PRIVACIDADE DE APLICATIVOS MÓVEIS DO GOVERNO BRASILEIRO

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre em Informática no Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, da Universidade Federal do Paraná.

Área de concentração: *Ciência da Computação*.

Orientador: Prof. Dr. Fabiano Silva.

CURITIBA PR

2022

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)
UNIVERSIDADE FEDERAL DO PARANÁ
SISTEMA DE BIBLIOTECAS – BIBLIOTECA CIÊNCIA E TECNOLOGIA

Costa, Carlos Humberto Lopes.
Análise de segurança e privacidade de aplicativos móveis do governo brasileiro. / Carlos Humberto Lopes Costa. – Curitiba, 2022.
1 recurso on-line : PDF.

Dissertação (Mestrado) – Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-Graduação em Informática.
Orientador: Prof. Dr. Fabiano Silva.

1. Informática. 2. Aplicativos móveis. 3. Segurança, Sistemas de. 4. Governo - Brasil. I. Silva, Fabiano. II. Universidade Federal do Paraná. Programa de Pós-Graduação em Informática. III. Título.

Bibliotecário: Nilson Carlos Vieira Júnior CRB-9/1797

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação INFORMÁTICA da Universidade Federal do Paraná foram convocados para realizar a arguição da Dissertação de Mestrado de **CARLOS HUMBERTO LOPES COSTA** intitulada: **ANÁLISE DE SEGURANÇA E PRIVACIDADE DE APLICATIVOS MÓVEIS DO GOVERNO BRASILEIRO**, sob orientação do Prof. Dr. FABIANO SILVA, que após terem inquirido o aluno e realizada a avaliação do trabalho, são de parecer pela sua APROVAÇÃO no rito de defesa.

A outorga do título de mestre está sujeita à homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela banca e ao pleno atendimento das demandas regimentais do Programa de Pós-Graduação.

CURITIBA, 24 de Outubro de 2022.

Assinatura Eletrônica
24/10/2022 15:08:00.0
FABIANO SILVA
Presidente da Banca Examinadora

Assinatura Eletrônica
05/11/2022 15:39:07.0
ALTAIR OLIVO SANTIN
Avaliador Externo (PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ)

Assinatura Eletrônica
28/10/2022 15:40:42.0
ANDRÉ RICARDO ABED GRÉGIO
Avaliador Interno (UNIVERSIDADE FEDERAL DO PARANÁ)

Em um mundo cada vez mais conectado, dedico este trabalho a todos que acreditam que privacidade não é sobre ter algo a esconder, mas, sim, a proteger. E àqueles que acreditam que é possível construir um país onde os dados pessoais são devidamente protegidos e a privacidade do cidadão é respeitada.

AGRADECIMENTOS

À vida por me proporcionar saúde, sabedoria e o encontro com pessoas fundamentais em minha vida.

Ao programa de Pós-Graduação em Informática (PPGInf) da Universidade Federal do Paraná (UFPR), seu corpo docente, funcionários e secretaria, pela atenção com seus discentes, organização e empenho, mesmo com a convivência restrita em meio ao cenário pandêmico entre 2020 e 2022.

A Polícia Científica do Paraná pelo apoio neste trabalho e pelos serviços prestados a toda sociedade paranaense, mesmo diante de tantos desafios.

Ao Professor Doutor Fabiano Silva, meu orientador, por topar o desafio em uma área de pesquisa distinta. Seu voto de confiança e suas contribuições e críticas, sempre muito pertinentes, foram fundamentais no amadurecimento deste trabalho.

Ao Professor Doutor André Grégio pelos conselhos, profissionalismo e por suas contribuições científicas à segurança da informação.

A toda minha família, em especial aos meus pais (Suely e Lineu) e a minha irmã (Pricilla), por todo amor, apoio, respeito, ensinamentos e por jamais medirem esforços para me proporcionar a melhor educação. Meus maiores orientadores na vida e os maiores incentivadores das realizações dos meus sonhos. Gratidão eterna.

A minha paixão (Lorena), esposa, companheira, namorada, amiga, pela paciência, incentivo, respeito, amor, confiança e por quem tenho muita admiração. Obrigado por me fazer muito feliz nesses quase 20 anos de companheirismo. E à sua família, na qual sempre fui recebido com muito afeto e tenho apoio inestimável.

RESUMO

Os dispositivos móveis e aplicativos impactaram a forma como nos comunicamos nos últimos anos. Seja para uso pessoal ou para trabalho, essas ferramentas tornaram-se cada vez mais indispensáveis no nosso cotidiano. A apropriação dessas novas tecnologias pela sociedade exigiu a adaptação dos órgãos governamentais. Consequentemente, o governo brasileiro passou a disponibilizar informações e serviços através de aplicativos móveis. Documentos oficiais como Cadastro de Pessoa Física (CPF), Carteira Nacional de Habilitação (CNH), Carteira de Trabalho, Título de Eleitor e Certificado de Registro e Licenciamento do Veículo (CRLV) já podem ser utilizados de forma digital, no celular, com a mesma validade dos documentos físicos. O governo brasileiro já disponibiliza centenas de aplicativos nas lojas de aplicativos das empresas Google e Apple, sendo que muitos desses aplicativos lidam com dados pessoais e confidenciais.

Este estudo avaliou quatorze critérios de segurança e privacidade de trinta aplicativos móveis do governo brasileiro, que totalizam mais de 93,5 milhões de downloads e representam mais de 95,8% dos downloads da loja oficial do governo federal na Google Play Store. O estudo apontou em detalhes que nenhum dos aplicativos atendeu todos os critérios de segurança e privacidade estabelecidos, sendo expostos diversos dados sensíveis do usuário, como: números de documentos, número de telefone, tipo sanguíneo, endereço, dados profissionais e de saúde, entre outros, além de solicitarem permissões para acessar dados desnecessários do usuário e/ou compartilharem dados sensíveis com serviços de terceiros, sem o claro consentimento do usuário.

O estudo evidenciou a necessidade de aprimorar os mecanismos de segurança dos aplicativos do governo brasileiro, pois, atualmente, representam um risco à privacidade de milhões de usuários brasileiros. Diante dos resultados da pesquisa e das recomendações propostas à Administração Pública Federal e aos usuários dos aplicativos do governo, busca-se contribuir para a construção de um país onde os dados pessoais são devidamente protegidos e a privacidade do cidadão é respeitada.

Palavras-chave: Segurança de Aplicativos Móveis; Privacidade; Vulnerabilidade; Governo;

ABSTRACT

Mobile devices and apps have impacted the way we communicate in recent years. Whether for personal use or for work, these tools have become increasingly indispensable in our daily lives. The appropriation of these new technologies by society required the adaptation of government agencies. Consequently, the Brazilian government started to make information and services available through mobile applications. National official documents such as Identification Cards, Driver's Licenses, Vehicle Registration and Licensing Certificates, Employment Cards and Voter IDs can now be used digitally, on cell phones, with the same validity as physical documents. The Brazilian government already makes hundreds of apps available in the app stores of Google and Apple, and many of these apps deal with personal and confidential data.

This study evaluated fourteen security and privacy criteria of thirty Brazilian government mobile applications, which total more than 93.5 million downloads and represent more than 95.8% of downloads from the official federal government store on the Google Play Store. The study pointed out in detail that none of the applications met all the established security and privacy criteria, exposing various sensitive user data, such as document numbers, telephone numbers, blood type, address, professional and health data, among others. The work also observed that the applications requested permissions to access unnecessary user data and/or shared sensitive data with third-party services, without the user's clear consent.

The study highlighted the need to improve the security mechanisms of Brazilian government applications, as they currently represent a risk to the privacy of millions of Brazilian users. Because of the research results and the proposed recommendations to the Federal Public Administration and the users of government applications, the aim is to contribute to the construction of a country where personal data is protected and the citizen's privacy is respected.

Keywords: Mobile Application Security; Privacy; Vulnerability; Government;

LISTA DE FIGURAS

2.1 Diagrama do modelo de ameaça dos aplicativos analisados. 26

3.1 Ataque *Man in the Middle* (MitM) à comunicação SSL/TLS. 41
3.2 Método de análise dos aplicativos utilizado neste estudo. 48

4.1 Banco de dados SQLite contendo número de CPF e senha do usuário em texto claro (não criptografados). 53
4.2 Arquivo XML contendo diversos dados do usuário em texto claro (não criptografados). 53
4.3 Arquivo PDF (encontrado no cartão de memória) contendo diversos dados do usuário em texto claro. 54
4.4 Requisição HTTPS contendo dados do usuário e com ausência de controle de cache. 54
4.5 Log do sistema móvel Android com dados sensíveis do usuário, registrados por um dos aplicativos. 55
4.6 Log do sistema móvel Android com dados sensíveis do usuário, registrados por um dos aplicativos. 55
4.7 Log do sistema móvel Android com login e senha do usuário, registrados por um dos aplicativos. 56
4.8 Qtd. de Permissões Perigosas por Aplicativo. 58
4.9 Qtd. Aplicativos que solicitaram determinada "Permissão Perigosa". 59
4.10 Log do sistema móvel Android contendo dados coletados do dispositivo pelo aplicativo "A24". 59
4.11 Aplicativo compartilhando dados do dispositivo do usuário com o serviço *OneSignal*. 61
4.12 Qtd. de Rastreadores por Aplicativo. 62
4.13 Qtd. de Aplicativos que utilizaram determinado Rastreador. 63
4.14 Contratação de serviço estrangeiro para desenvolvimento de aplicativo móvel do governo brasileiro. 65

LISTA DE TABELAS

2.1 Dimensões das iniciativas de Governo Móvel (Oui-Suk, 2010). 16
2.2 Classificação dos aplicativos móveis governamentais, segundo (Ganapati, 2015). 16
2.3 Modelo de ameaça para os aplicativos analisados. 27

3.1 Aplicativos móveis selecionados e número de downloads. 36
3.2 Critérios avaliados de segurança e privacidade. 38

4.1 Alguns dados sensíveis armazenados sem a devida proteção. 57
4.2 Resumo das permissões perigosas solicitadas pelos aplicativos. 60
4.3 Resumo dos rastreadores existentes nos aplicativos. 64
4.4 Resumo da análise dos aplicativos móveis do governo brasileiro (aplicativos A1 a A15). 66
4.5 Resumo da análise dos aplicativos móveis do governo brasileiro (aplicativos A16 a A30). 67

5.1 Mitigação das ameaças de adversários por meio de recomendações aos usuários.. 76

LISTA DE ACRÔNIMOS

CDT	Carteira Digital de Trânsito
CNH	Carteira Nacional de Habilitação
CNPJ	Cadastro Nacional da Pessoa Jurídica
CNS	Carteira Nacional de Saúde
CPF	Cadastro de Pessoas Físicas
CRLV	Certificado de Registro e Licenciamento do Veículo
DAS	Documento de Arrecadação do Simples Nacional
IMEI	International Mobile Equipment Identity
INSS	Instituto Nacional do Seguro Social
IRPF	Imposto de Renda da Pessoa Física
MobSF	Mobile Security Framework
NIT	Número de Identificação do Trabalhador
PIS	Programa de Integração Social
RENAVAM	Registro Nacional de Veículos Automotores
RG	Registro Geral (Carteira de Identidade)
OWASP	Open Web Application Security Project
SUS	Sistema Único de Saúde
XML	Extensible Markup Language

SUMÁRIO

1 INTRODUÇÃO 12
1.1 MOTIVAÇÃO 13
1.2 OBJETIVO DE PESQUISA 13
1.3 CONSIDERAÇÕES LEGAIS 13
1.4 NOTIFICAÇÃO DE VULNERABILIDADES E SIGILO DOS APLICATIVOS . 14
1.5 ORGANIZAÇÃO DA DISSERTAÇÃO 14
2 FUNDAMENTOS E TRABALHOS RELACIONADOS 15
2.1 GOVERNO MÓVEL 15
2.2 APLICATIVOS MÓVEIS DO GOVERNO BRASILEIRO 17
2.3 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) 18
2.4 VULNERABILIDADES EM APLICATIVOS MÓVEIS 19
2.5 COMPORTAMENTOS INSEGUROS DOS USUÁRIOS 21
2.6 MODELO DE AMEAÇA 23
2.7 ANÁLISE DE SEGURANÇA DE APLICATIVOS MÓVEIS 29
2.8 TRABALHOS RELACIONADOS 31
3 MÉTODO 36
3.1 SELEÇÃO DOS APLICATIVOS DO GOVERNO BRASILEIRO 36
3.2 CRITÉRIOS AVALIADOS DE SEGURANÇA E PRIVACIDADE 37
3.2.1 Arquivo de Manifesto 37
3.2.2 Armazenamento de Dados 39
3.2.3 Transmissão de Dados 40
3.2.4 Permissões Perigosas 42
3.2.5 Outros riscos 42
3.3 CONFIGURAÇÃO DO AMBIENTE DE TESTE 44
3.3.1 Dispositivo *host* 44
3.3.2 Dispositivo móvel de teste 44
3.3.3 Configuração de Rede 45
3.4 FERRAMENTAS UTILIZADAS 45
3.5 MÉTODO DE ANÁLISE 47
3.5.1 Busca por dados sensíveis 49
3.5.2 Problemas na busca por palavras-chave 50
4 RESULTADOS E DISCUSSÃO 52
5 CONCLUSÃO 69
5.1 RESPOSTAS ÀS PERGUNTAS DE PESQUISA 69
5.2 RECOMENDAÇÕES À ADMINISTRAÇÃO PÚBLICA FEDERAL 70

5.3 RECOMENDAÇÕES AOS USUÁRIOS DOS APLICATIVOS MÓVEIS. 72
5.4 PRINCIPAIS CONTRIBUIÇÕES DA PESQUISA 77
5.5 TRABALHOS FUTUROS 77
REFERÊNCIAS 78
APÊNDICE A – RELATÓRIO DETALHADO DE ANÁLISE 84

1 INTRODUÇÃO

A cada dia mais poderosos, os *smartphones* estão se tornando a principal plataforma de computação e comunicação. Esses dispositivos móveis contam com aplicativos para as mais variadas necessidades, como comunicação instantânea, troca de e-mails, fazer pesquisas, assistir filmes, escutar músicas, entre outras atividades básicas do dia a dia. Eles são consideravelmente mais práticos do que computadores e notebooks, já que estão sempre conosco, e até mais versáteis em muitas tarefas. Segundo a pesquisa "TIC Domicílios 2019", o número de residências brasileiras com computador reduziu para 39% — era de 50% em 2016 (Comitê Gestor da Internet do Brasil - CGI.br, 2019). A pesquisa cita ainda que a principal forma de acesso à Internet tem sido através de dispositivos móveis, especialmente nas famílias brasileiras de rendas mais baixas. A pesquisa aponta que 58% dos brasileiros acessam a Internet exclusivamente pelo celular, e na área rural esse número sobe para 79%. Nas classes D/E, o aparelho celular é um grande fator de inclusão social, sendo o único acesso à Internet para 85% dessa população.

O crescimento explosivo de usuários de dispositivos e aplicativos móveis exigiu a adequação do setor público. Observou-se a possibilidade de utilizar esses recursos como forma de ampliar o acesso a serviços públicos, não apenas para uma parte da população mais vulnerável, como também para aqueles que estão longe dos grandes centros urbanos. Nos últimos anos, o governo brasileiro ampliou o número de aplicativos móveis que disponibilizam informações e oferecem serviços aos cidadãos. Documentos oficiais como Cadastro de Pessoa Física (CPF), Carteira Nacional de Habilitação (CNH), Carteira de Trabalho e Título de Eleitor já podem ser utilizados de forma digital com a mesma validade dos documentos físicos. A partir de junho de 2020 (Deliberação Contran nº 180, 2019), todos os estados brasileiros deixaram de emitir a versão impressa do Certificado de Registro e Licenciamento de Veículo (CRLV), que foi substituído pela versão em meio eletrônico (CRLV-e), acessível através do aplicativo móvel "Carteira Digital de Trânsito – CDT" e disponível para download nas principais lojas de aplicativos. Atualmente, o governo brasileiro já disponibiliza centenas de aplicativos nas lojas oficiais das empresas Google e Apple.

Muitos destes aplicativos móveis do governo brasileiro lidam com dados pessoais e confidenciais, tais como número de RG, CPF, telefone, endereço residencial, localização, dados de saúde e renda, entre outros. Estes aplicativos podem ainda utilizar os sensores dos dispositivos para coletar outros dados dos usuários, muitas vezes sem o seu consentimento, introduzindo riscos significativos à privacidade. Desta forma, considerando que os dispositivos móveis carregam um volume cada vez maior de informações e que, devido a sua portabilidade, são difíceis de proteger fisicamente, sendo muitas vezes alvos de roubo e furto, o armazenamento de dados pessoais e confidenciais nestes equipamentos se tornou um problema crítico, exigindo o aprimoramento da segurança dos aplicativos pelos desenvolvedores.

1.1 MOTIVAÇÃO

A crescente adoção de aplicativos móveis pelo setor público — sendo utilizados inclusive como "documento de identificação" oficial, a Lei Geral de Proteção de Dados Pessoais (LGPD), que passou a vigorar em 2020, a diversidade de vulnerabilidades que podem comprometer a segurança destes aplicativos e o comportamento inseguro dos usuários são as principais motivações desta pesquisa, e serão abordadas em detalhes nos capítulos seguintes. Deste modo, torna-se fundamental determinar se é possível confiar nos aplicativos móveis do governo brasileiro, ou se eles representam um risco à privacidade dos cidadãos brasileiros. Espera-se que esta pesquisa produza conhecimento científico capaz de contribuir para a construção de um país onde os dados pessoais são devidamente protegidos pelos aplicativos móveis de governo e o respeito à privacidade do cidadão é reconhecido.

1.2 OBJETIVO DE PESQUISA

O objetivo desta pesquisa é responder às seguintes perguntas:

A **Os dados pessoais e confidenciais dos usuários de aplicativos móveis do governo brasileiro podem ser expostos?**

B **Esses aplicativos móveis coletam dados desnecessários ou compartilham informações dos usuários brasileiros sem o devido consentimento?**

Para alcançar esse objetivo, será necessário o conhecimento de vulnerabilidades e comportamentos que afetam a segurança e a privacidade de aplicativos móveis bem como de técnicas e ferramentas para análise desses aplicativos.

1.3 CONSIDERAÇÕES LEGAIS

Durante os experimentos desta pesquisa, pode ser necessário fazer a engenharia reversa dos aplicativos analisados, com propósito de reconstruir os artefatos do aplicativo. Portanto, algumas considerações legais importantes devem ser levadas em consideração.

Engenharia reversa é a atividade de tentar entender como um produto (um dispositivo, um programa, etc.) funciona, o que ele faz exatamente e como se comporta em diversas circunstâncias. No Brasil não existe lei específica que autorize ou proíba a realização de engenharia reversa de programas ou aplicativos móveis. A Lei 9.609/1998, conhecida como "Lei de Software", dispõe sobre a proteção da propriedade intelectual de programas de computador. Em suma, esta lei criminaliza quem "*violar direitos de autor de programa de computador*", conforme artigo 12. Em uma perspectiva mais ampla, há ainda a Lei 9.610/1998, que consolida a legislação nacional sobre direitos autorais.

Porém, em nenhum momento haverá qualquer modificação, reprodução ou distribuição dos aplicativos analisados nesta pesquisa, que possa incorrer em violação à direitos autorais. O motivo para obter uma aproximação do código-fonte original é entender, estudar e observar melhor o comportamento dos aplicativos.

Este estudo é para fins acadêmicos e espera-se que as descobertas ajudem o governo brasileiro a adotar metodologias de desenvolvimento seguro para a proteção da segurança e privacidade dos dados do cidadão.

1.4 NOTIFICAÇÃO DE VULNERABILIDADES E SIGILO DOS APLICATIVOS

Cumpre referir que as vulnerabilidades reveladas nesta pesquisa, que possam levar a exposição de dados sensíveis do usuário ou do aplicativo, foram documentadas e encaminhadas para o e-mail do responsável pelo aplicativo móvel, indicado na Google Play Store. Além da notificação do responsável pelo aplicativo, foi dado um prazo para correção das vulnerabilidades. A publicação desta pesquisa ocorrerá após 90 (noventa) dias da notificação das vulnerabilidades aos desenvolvedores.

A pesquisa será publicada com os nomes dos aplicativos anonimizados, de modo a dificultar a identificação dos aplicativos e suas vulnerabilidades pelos leitores. O relatório detalhado das vulnerabilidades constam no Apêndice A, desta pesquisa, o qual será mantido em sigilo na Universidade Federal do Paraná pelo período de 6 (seis) meses após a publicação deste trabalho.

1.5 ORGANIZAÇÃO DA DISSERTAÇÃO

Os capítulos seguintes desta Dissertação foram assim organizados, no Capítulo 2 está a fundamentação teórica necessária ao desenvolvimento da pesquisa e alguns trabalhos relacionados. No Capítulo 3 são apresentados os critérios de segurança e privacidade avaliados, o método e os instrumentos utilizados na investigação. No Capítulo 4 são apresentados e discutidos os resultados da análise dos critérios de segurança e privacidade para os aplicativos móveis do governo brasileiro. Finalmente, no Capítulo 5, são expostas as conclusões, com as respostas às perguntas de pesquisa, são realizadas recomendações à Administração Pública e aos usuários dos aplicativos e, por fim, são apresentadas as principais contribuições da pesquisa e propostos alguns trabalhos futuros. O Apêndice A apresenta o relatório detalhado da análise de cada um dos aplicativos selecionados e será mantido em sigilo por um período definido, conforme discutido na seção anterior.

2 FUNDAMENTOS E TRABALHOS RELACIONADOS

Neste Capítulo é apresentada a fundamentação teórica necessária ao desenvolvimento da pesquisa. É relevante: a compreensão da utilização da tecnologia móvel pelo setor público, abordada na Seção 2.1; a utilização de aplicativos móveis pelo governo brasileiro, na Seção 2.2; considerações sobre a Lei Geral de Proteção de Dados Pessoais, na Seção 2.3; as vulnerabilidades mais comuns dos aplicativos móveis, descritas na Seção 2.4; os comportamentos inseguros dos usuários que afetam a segurança dos aplicativos, discutidos na Seção 2.5; o modelo de ameças de aplicativos móveis, apresentados na Seção 2.6; os conceitos relacionados à análise de segurança de aplicativos, abordados na Seção 2.7; e alguns trabalhos relacionados ao objeto de estudo desta pesquisa, que seguem na Seção 2.8.

2.1 GOVERNO MÓVEL

O crescimento do uso de dispositivos e aplicativos móveis criou novas oportunidades para o setor público, dando origem ao conceito de Governo Móvel. Knopp (2005) define Governo Móvel como "*uma aplicação local flexível de tecnologia de informação e comunicação eletrônica para permitir a comunicação com ou dentro do governo e administração por meio de dispositivos móveis e sem pontos de acesso fixos*"[1]. Esse conceito se distingue de Governo Eletrônico, enquanto este permite o acesso a serviços eletrônicos públicos a qualquer hora, o Governo Móvel permite acesso aos serviços governamentais a qualquer hora e "em qualquer lugar" (Ganapati, 2015). Um estudo da empresa Google, em parceria com a empresa Brain & Company, revelou que quase 60% dos usuários brasileiros de *smartphone* utilizam o aparelho para ter acesso a serviços públicos (Google e Brain & Company, 2020). Muitos desses serviços são oferecidos através de aplicativos móveis.

Aplicativos móveis são programas projetados especificamente para dispositivos móveis, que geralmente combinam recursos de computação e comunicação. Os aplicativos podem ainda tirar proveito dos recursos de hardware de um dispositivo móvel, como dos recursos de câmera e de posicionamento global (GPS). Esses aplicativos estão disponíveis em lojas de aplicativos dos principais fornecedores de sistemas móveis, tais como Play Store, da empresa Google, e App Store, da Apple. Essas lojas são cruciais para centralizar a consulta e a instalação de aplicativos. O Governo do Brasil já conta com dezenas de aplicativos móveis, os quais serão discutidos em mais detalhes na Seção 2.2.

[1]Mobile Government stands for a local flexible application of electronic information and communication technology to enable communication with or within government and administration by means of mobile devices and without fixed access points.

Na publicação "Introduction of m-Government & IT Convergence Technology", Oui-Suk (2010) estabelece uma classificação para aplicativos móveis governamentais. Segundo o autor, as iniciativas de governo móvel podem ser avaliadas a partir de duas dimensões fundamentais: considerando o tipo de público (individual ou organização) e o tipo de uso (interno ou externo), conforme tabela 2.1.

Tabela 2.1: Dimensões das iniciativas de Governo Móvel (Oui-Suk, 2010).

	INDIVIDUAL	ORGANIZAÇÃO
USO INTERNO	Governo Móvel para Servidores (mG2E) Refere-se ao uso das tecnologias móveis por parte de servidores públicos ou funcionários a serviços do governo	Governo Móvel para Governos (mG2G) Refere-se ao uso das tecnologias móveis para aprimorar a interação entre agências governamentais
USO EXTERNO	Governo Móvel para Cidadão (mG2C) Aprimoramento da interação entre instituições públicas e cidadão por meio das tecnologias móveis	Governo Móvel para Empresas (mG2B) Uso das tecnologias móveis para melhorar a interação entre instituições públicas e organizações do setor privado

Em um publicação mais recente, no relatório produzido para a "IBM Center for The Business of Government", Sukumar (Ganapati, 2015) simplifica a classificação anterior em dois grupos, conforme tabela 2.2. Segundo o autor, o primeiro grupo é composto por aplicativos voltados à própria instituição, são aqueles dirigidos apenas ao uso interno das instituições públicas. O propósito principal é melhorar a produtividade dos servidores dos órgãos públicos. Já o segundo grupo abrange os aplicativos voltados para o cidadão. São aqueles acessíveis a qualquer pessoa que queira utilizar um serviço do governo. Nesse último grupo, o objetivo é utilizar novas tecnologias para aprimorar a relação entre a administração pública e a sociedade.

Tabela 2.2: Classificação dos aplicativos móveis governamentais, segundo (Ganapati, 2015).

USO INTERNO	Voltado a própria Instituição (melhoria da produtividade dos órgãos)
USO EXTERNO	Voltado ao Cidadão (aprimorar a relação dos órgãos com a sociedade)

Considerando a classificação proposta por Ganapati (2015), esta pesquisa analisará a segurança e a privacidade dos aplicativos móveis de uso externo, ou seja, aqueles aplicativos acessíveis por qualquer pessoa que queira utilizar um serviço móvel do governo brasileiro.

2.2 APLICATIVOS MÓVEIS DO GOVERNO BRASILEIRO

Considerando a tendência do Governo Móvel, em maio de 2021, foi identificado que o governo brasileiro já disponibilizava 150 aplicativos móveis em sua conta na loja de aplicativos Google Play Store.

O Governo do Brasil disponibiliza aplicativos de diferentes segmentos e áreas de governo, como na área de Previdência Social ("Meu INSS"), na área de Renda e Tributação ("Meu Imposto de Renda"), na área de Educação ("ENEM"), na área de Saúde ("Conecte SUS"), na área de Segurança Pública ("Sinesp Cidadão"), entre outras. No momento desta pesquisa, os aplicativos do Governo Federal já acumulavam mais de 267 milhões de downloads e mais de 8,5 milhões de avaliações. Esses aplicativos estavam centralizados na conta "Governo do Brasil"[2], na Google Play Store.

A centralização de aplicativos do Governo Federal decorre da Portaria nº 39, de 09/07/2019, do Ministério da Economia, que estabelece que o registro de aplicativos móveis nas lojas de aplicativos será realizado por meio de conta única de publicação do Governo Federal. Nesta conta única serão mantidos todos os aplicativos de órgãos do governo brasileiro. A disponibilização de aplicativos por meio de uma conta única do Governo Federal é um importante critério de segurança, pois facilita a busca por aplicativos oficiais pelo cidadão. Anteriormente a centralização, os aplicativos do governo brasileiro estavam distribuídos nas contas de desenvolvedor de cerca de 43 órgãos públicos do Brasil, segundo Neto (2020).

Alguns documentos oficiais brasileiros já foram disponibilizados de forma digital, através de aplicativos, como: Cadastro de Pessoa Física (CPF), Carteira Nacional de Habilitação (CNH), Carteira de Trabalho e Título de Eleitor, que podem ser utilizados com a mesma validade dos documentos físicos. O Certificado de Registro e Licenciamento de Veículo (CRLV), documento veicular impresso e obrigatório para todos os veículos automotores em circulação, deixou de ser emitido por todos os estados brasileiros desde junho de 2020 e pode ser substituído pela sua versão em meio eletrônico, acessível através do aplicativo móvel "Carteira Digital de Trânsito".

A pandemia do Covid-19 também contribuiu para tornar o *smartphone* uma importante porta de acesso aos serviços governamentais. A exemplo, o programa de Auxílio Emergencial do governo federal brasileiro foi disponibilizado como um processo 100% digital. O Auxílio Emergencial é um benefício financeiro concedido pelo Governo Federal destinado aos trabalhadores informais, microempreendedores individuais (MEI), autônomos e desempregados, e tem por objetivo fornecer proteção emergencial no período de enfrentamento à crise causada pela pandemia do novo coronavírus. Por meio do aplicativo "CAIXA Tem", o cidadão cadastra o seu número de CPF, acompanha o status de aprovação e a disponibilização do benefício e recebe o valor do auxílio automaticamente, por meio de uma conta digital no próprio aplicativo. Por fim, o beneficiário pode ainda fazer pagamentos e compras com um cartão de débito virtual, sem a necessidade de ir pessoalmente à agências bancárias.

[2]https://play.google.com/store/apps/dev?id=5829287075355252046

2.3 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Em 2018, foi aprovada no Brasil a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), que entrou em vigor posteriormente, em 18 de setembro de 2020. A lei representa um marco histórico na regulamentação sobre o tratamento de dados pessoais no Brasil, tanto em meios físicos quanto em plataformas digitais, incluindo aplicativos móveis. A LGPD é destinada tanto a instituições privadas como públicas, portanto, deve ser seguida por União, estados, Distrito Federal e municípios (Supremo Tribunal Federal, 2021). Considera-se tratamento toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, entre outras.

De acordo com a LGPD (Lei 13.709/2018, art. 6º), as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

i. **finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular (pessoa a quem se referem os dados pessoais), sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

ii. **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

iii. **necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

iv. **livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

v. **qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

vi. **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

vii. **segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

viii. **prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

ix. **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

x. **responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Diante do exposto, destacam-se os princípios da segurança, prevenção, necessidade e transparência. O princípio da segurança assegura aos titulares o direito à segurança dos dados, por parte dos agentes de tratamento, de utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. O princípio da prevenção assegura aos titulares o direito à adequada prevenção de danos, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. O princípio da necessidade assegura aos titulares o direito à limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento. Já o princípio da transparência assegura aos titulares o direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento (Governo do Brasil, 2021a).

Considerando que os aplicativos do governo brasileiro manipulam informações potencialmente confidenciais, tais princípios, assim como todos os demais, devem balizar o desenvolvimento de aplicativos móveis da Administração Pública Federal.

2.4 VULNERABILIDADES EM APLICATIVOS MÓVEIS

A maioria dos aplicativos contemporâneos usam e armazenam dados pessoais. Em junho de 2019, a empresa de segurança móvel NowSecure testou 250 aplicativos populares para Android e descobriu que cerca de 70% dos aplicativos vazavam dados pessoais confidenciais (Reed, 2019). Para obter dados confidenciais dos usuários, os adversários[3] exploram diferentes tipos de vulnerabilidades nos aplicativos. Portanto, é importante que os desenvolvedores compreendam quais são essas vulnerabilidades e como tratá-las. Uma ferramenta essencial para o desenvolvimento seguro de aplicativos móveis é o documento OWASP Mobile Top Ten 2016 (OWASP, 2016). O documento identifica os dez principais tipos de riscos de segurança enfrentados por aplicativos móveis em todo o mundo.

[3]Adversário: uma entidade que não está autorizada a acessar ou modificar informações, ou que trabalha para anular quaisquer proteções concedidas às informações (Paulsen e Byers, 2019).

Segundo o OWASP Mobile Top Ten 2016, os dez principais riscos enfrentados por aplicativos móveis, identificados de M1 a M10, são brevemente descritos abaixo:

- **M1: Uso impróprio da plataforma** - Esta categoria cobre o uso indevido de um recurso da plataforma ou falha no uso dos controles de segurança da plataforma. Pode incluir intenções do Android, permissões de plataforma, uso indevido de TouchID, Keychain ou algum outro controle de segurança que faça parte do sistema operacional móvel;

- **M2: Armazenamento de dados inseguro** - Esta categoria abrange o armazenamento de dados sem a devida preocupação com segurança e privacidade. No caso de um adversário ter acesso físico a um dispositivo móvel, por exemplo perdido ou roubado, ele pode obter informações de identificação pessoal e outros dados confidenciais. Um adversário pode ainda construir um *malware* ou modificar um aplicativo legítimo para obter acesso a tais informações.

- **M3: Comunicação Insegura** - Esta categoria trata da falha de proteção do tráfego de rede pelos aplicativos. Um adversário pode explorar essa vulnerabilidade para interceptar dados confidenciais enquanto eles estão trafegando pela rede;

- **M4: Autenticação Insegura** - Muitos aplicativos móveis executam um processo de autenticação, antes que os usuários possam executar qualquer ação no aplicativo. Esta categoria aborda adversários que exploram falhas na autenticação de usuários ou no gerenciamento de sessões, permitindo que um usuário anônimo execute ações não autenticadas, podendo prejudicar usuários legítimos ou o próprio sistema.

- **M5: Criptografia Insuficiente** - Esta categoria se refere à utilização de algoritmos criptográficos inseguros ou falhas no processo de criptografia, resultando na recuperação não autorizada de informações confidenciais por um adversário;

- **M6: Autorização Insegura** - O problema de autorização tem uma relação próxima com o problema da autenticação, e às vezes são combinados. Falhas de autorização podem resultar no acesso não autorizado a dados ou recursos.

- **M7: Código de baixa qualidade** - Esta categoria versa sobre as vulnerabilidades decorrentes de práticas de programação de código de baixa qualidade, como injeção de código e estouro de buffer;

- **M8: Adulteração de código** - Esta categoria aborda a possibilidade de adversários poderem adulterar aplicativos para executar algumas ações que não foram planejadas para o aplicativo original. Neste caso, os aplicativos móveis são executados em um ambiente que não está sob o controle da organização que o desenvolveu;

- **M9: Engenharia Reversa** - Esta categoria trata do uso da técnica de engenharia reversa para analisar o código-fonte do aplicativo. Através dessa técnica, um adversário pode ter obter informações importantes sobre um aplicativo, como algoritmos, criptografia utilizada, informações sobre o servidor remoto e outras informações valiosas;
- **M10: Funcionalidade estranha** - Esta categoria cobre as funcionalidades ocultas e códigos de teste deixados pelos desenvolvedores do aplicativo, que podem ser utilizados por um adversário para realização de ataque.

2.5 COMPORTAMENTOS INSEGUROS DOS USUÁRIOS

Para aprimorar os mecanismos de segurança dos aplicativos móveis é importante também que os desenvolvedores compreendam e considerem que muitos usuários adotam comportamentos inseguros no uso de seus dispositivos. Embora muitos usuários de *smartphones* tomem algumas medidas de segurança, cerca de 24% deles ainda ignoram riscos potenciais (Stylios et al., 2016). A maioria dos usuários habilita a funcionalidade de bloqueio de tela para proteger seus telefones do acesso físico; no entanto, eles desconsideram outras práticas recomendadas de segurança, por exemplo, usar uma VPN ao se conectar a um WiFi público ou desligar recursos não utilizados no dispositivo (Breitinger et al., 2020).

Em comparação com os computadores, os *smartphones* possuem maior probabilidade de serem perdidos ou roubados. Estima-se que 64 milhões de brasileiros já foram vítimas de roubo ou furto de celular, totalizando 102,4 milhões de aparelhos, segundo a pesquisa "Roubo de celulares no Brasil - Julho/2020" (Mobile Time e Opinion Box, 2020). Dos entrevistados, 50% declararam já terem tido um celular roubado ou furtado. Um adversário que se apodere desse dispositivo poderá ter acesso aos dados confidenciais armazenados no equipamento.

O nível mais básico de proteção que se deve ter em um dispositivo móvel é o bloqueio de tela. Sem ele, qualquer pessoa pode acessar os dados pessoais do usuário, incluindo os dados de aplicativos de governo, que podem conter informações altamente confidenciais. Os dispositivos oferecem diversos métodos para bloqueio de tela, como código numérico (PIN[4]), senha alfanumérica, padrão geométrico, e, em dispositivos mais modernos, impressão digital e reconhecimento facial, além de outros métodos ainda não utilizados em larga escala. Segundo pesquisa da empresa de produtos de segurança AVAST, 95% dos brasileiros utilizam senhas fracas, o próprio nome, nome do cachorro e a própria data de aniversário são alguns exemplos de senhas comumente utilizadas (AVAST, 2018). Um número considerável de usuários do Android preferem o padrão de desbloqueio em vez de PINs ou senhas textuais. Porém, os usuários preferem usar um padrão geométrico simples ao invés de um mais complexo, optando pela usabilidade e não pela segurança, tornando seus dispositivos vulneráveis (Andriotis et al., 2016) (Gil et al., 2018).

[4]Personal identification number

Com relação a biometria, este método de autenticação oferece uma maneira de desbloquear dispositivos móveis mais conveniente (não havendo a necessidade de memorizar códigos secretos) e segura (mais difícil de ser roubada), se comparada à utilização de senhas e padrões geométricos de desbloqueio. Esse meio de autenticação explora características biométricas humanas únicas, por exemplo, impressões digitais, padrões de íris e contorno facial. Em comparação com autenticações que utilizam senhas e padrões de desbloqueio, é muito mais difícil para um adversário atacar a autenticação baseada em biometria por meio de força bruta ou ataques de adivinhação. No entanto, a biometria ainda é vulnerável a alguns tipos de ataques, por exemplo, Maro e Kovalchuk (2018) descrevem em seu artigo como contornar a proteção biométrica por impressão digital sem a necessidade de ferramentas caras ou amostras de impressão digital de alta qualidade. Após a coleta de uma impressão digital, a técnica utiliza basicamente um programa de edição gráfica, as saliências do toner de impressão a laser e gelatina artificial. As impressões digitais artificiais foram utilizadas com sucesso para desbloquear os *smartphones* iPhone 6, iPhone 8 e Samsung Galaxy S8, além do *tablet* iPad Air 2.

As redes Wi-Fi públicas têm sido bastante utilizadas por usuários de *smartphones*, nota-se ainda que 58% dos brasileiros acessam a internet exclusivamente pelo celular (TIC Domicílios, 2019). As redes Wi-Fi públicas estão disponíveis em restaurantes, shoppings, mercados, e está cada vez mais fácil localizar novos pontos de acesso. Elas fornecem uma maneira conveniente e econômica de acessar a Internet. No entanto, essa liberdade tem um preço, e poucas pessoas realmente entendem os riscos associados a essas conexões públicas. Uma pesquisa da empresa Norton identificou que 58% dos brasileiros acreditam que suas informações pessoais estão seguras ao usar uma rede Wi-Fi pública e 90% colocam informações pessoais em risco, incluindo os detalhes de suas contas bancárias, ao transferir informações confidenciais por um Wi-Fi público (Norton, 2017).

Nem todo ponto de acesso público é confiável, mesmo aqueles que carregam o nome de uma empresa ou marca confiável. Segundo dados da pesquisa "Mobile Security Index 2021", 59% das empresas do setor de varejo (incluindo hotéis) identificaram pontos de acesso Wi-Fi desonestos usando a identidade de seus negócios (Verizon, 2021). Por um custo mínimo, um adversário pode obter equipamentos avançados o suficiente para criar um ponto de acesso falso, monitorar o tráfego online de usuários e aplicativos, capturando informações valiosas sobre eles.

O uso cada vez mais intenso dos dispositivos móveis também ocasionou o aumento no número de estações de carregamento em áreas públicas, como shoppings, aeroportos e terminais de ônibus. Embora esses locais ofereçam energia gratuita, não há garantia que a estação de carregamento não seja controlada de forma maliciosa. Uma forma de ataque para explorar esse canal de comunicação e roubar dados confidenciais dos usuários foi apresentada pela primeira vez por Wang e Stavrou (2010). Em novembro de 2019, a cidade de Los Angeles emitiu um alerta para os viajantes, informando que criminosos estão carregando *malware* em estações públicas de carregamento de dispositivos por USB, para maliciosamente acessar dispositivos eletrônicos enquanto eles estão sendo carregados (Los Angeles County District Attorney's Office, 2019).

A obtenção de direitos de acesso de superusuário, popularmente conhecido como *rooting*, tem sido cada vez mais comum entre os usuários que querem assumir o controle total de seus dispositivos. Segundo pesquisa do Kaspersky Lab, os motivos mais comuns pelos quais os usuários fazem *rooting* em seus dispositivos Android são obter acesso irrestrito ao sistema de arquivos, melhorar o desempenho do dispositivo, instalar diferentes versões do sistema operacional, entre outros (Kaspersky Lab, 2017). Embora esse acesso tenha algumas vantagens potenciais, ele também apresenta desvantagens, pois viola um importante mecanismo de segurança do Android. Isso significa que a segurança do dispositivo está comprometida e que todos os aplicativos, incluindo os maliciosos, podem acessar os dados pertencentes a outros aplicativos (Samsung, 2019), possibilitando o vazamento de dados confidenciais. O National Institute of Standards and Technology (NIST) inclusive orienta que as organizações que gerenciam centralmente a segurança dos dispositivos móveis devem detectar dispositivos *rooting* e proibir o seu uso (Souppaya e Scarfone, 2013).

Portanto, há necessidade dos desenvolvedores de aplicativos móveis estarem atentos aos comportamentos inseguros dos usuários, de modo a adotarem mecanismos de segurança que mitiguem esses riscos e impossibilitem o comprometimento de dados pessoais e da privacidade dos usuários em seus aplicativos.

2.6 MODELO DE AMEAÇA

Nas seções anteriores apresentou-se os dez principais tipos de riscos de segurança enfrentados por aplicativos móveis, segundo o OWASP Mobile Top Ten 2016, e alguns comportamentos dos usuários que podem contribuir para a insegurança destes aplicativos. Nesta seção, será apresentado o modelo de ameaças utilizado neste estudo.

A modelagem de ameaças é uma tarefa estruturada para identificar e avaliar as ameaças e vulnerabilidades que podem comprometer um recurso; em termos simples, busca-se verificar o que poderia dar errado em um aplicativo (Velu, 2016). Segundo Tarandach e Coles (2020), a modelagem de ameaças é o processo de análise de um sistema para procurar pontos fracos que vêm da escolha de um design ruim. Ao realizar a modelagem de ameaças, o aplicativo é visto como uma coleção de seus componentes e suas interações com o mundo fora do aplicativo (como outros sistemas com os quais interage) e os atores que podem executar ações nesses sistemas. O objetivo é tentar identificar como esses componentes podem falhar ou serem levados a falhar.

Há muitas metodologias de modelagem de ameaças disponíveis, sendo destacadas em Velu (2016) e Tarandach e Coles (2020) as metodologias STRIDE, PASTA e Trike. No entanto, Tarandach e Coles (2020) ressaltam que não existe uma metodologia melhor que a outra. Uma metodologia específica funcionará com sucesso em algumas organizações e equipes, ou para tecnologias específicas ou requisitos de conformidade, mas falhará completamente em outras. A obra cita ainda que Adam Shostack, guru da modelagem de ameaças, disse que "*um bom modelo*

de ameaça é aquele que produz descobertas válidas". Entende-se por descobertas válidas aquelas que podem ser traduzidas em ações que permitam mitigar uma possível vulnerabilidade.

O modelo de ameaças deste estudo apoiou-se no processo de descoberta de ameaças apresentado por Kesäniemi e Mäkelä (2011), que decorre de cinco perguntas: *1. "O que queremos proteger e por quê?"; 2. "Onde o ataque poderia acontecer?"; 3. "O que poderia dar errado?"; 4. "Temos proteção adequada?"; 5. "Qual é o risco que aceitamos?"*. Deste modo, serão apresentados abaixo alguns possíveis cenários de ataque comuns aos aplicativos avaliados. O modelo de ameaças é apresentado na forma de diagrama, conforme a figura 2.1, e na forma de tabela, conforme a tabela 2.3.

Destacam-se os seguintes cenários de ataque:

- **Cenário 1** - Um adversário com acesso físico ao dispositivo pode obter dados privados do usuário, caso o aplicativo mantenha uma autenticação persistente, não exigindo uma nova autenticação a cada acesso ao aplicativo. O aplicativo confia exclusivamente nos controle de acesso do dispositivo (ex. bloqueio de tela);

- **Cenário 2** - Um adversário com acesso físico ao dispositivo pode obter dados privados do aplicativo e do usuário, mesmo que o aplicativo utilize um canal de comunicação seguro (*SSL/TLS*). Isto pode ocorrer caso o aplicativo confie em qualquer autoridade certificadora e seja instalado no dispositivo móvel o certificado de uma autoridade mal-intencionada, possibilitando um ataque *Man in the Middle* (MitM);

- **Cenário 3** - Um adversário com acesso físico ao dispositivo pode obter dados privados do usuário e do aplicativo, através da instalação de um aplicativo malicioso, podendo inclusive instalar uma versão maliciosa de um aplicativo já em uso pelo usuário;

- **Cenário 4** - Um adversário com acesso físico ao dispositivo pode obter dados privados do usuário e do aplicativo, caso o aplicativo armazene esses dados no dispositivo de armazenamento externo (cartão de memória) de forma insegura (não criptografados);

- **Cenário 5** - Uma dispositivo conectado fisicamente a uma estação maliciosa (controlada por um adversário) pode expor dados privados do usuário e do aplicativo por meio da funcionalidade de backup do aplicativo, caso esteja configurada de forma inapropriada. Uma estação maliciosa poderia, por exemplo, ser disponibilizada como uma estação pública para carregamento de dispositivos por USB.

- **Cenário 6** - Um dispositivo conectado fisicamente a uma estação maliciosa (controlada por um adversário) pode expor dados privados do usuário e do aplicativo, caso o aplicativo registre esses dados no *log* do sistema móvel Android;

- **Cenário 7** - Um dispositivo conectado fisicamente a uma estação maliciosa (controlada por um adversário) pode expor dados privados do usuário e do aplicativo em dispositivos *rooted*, caso o aplicativo armazene esses dados de forma insegura (não criptografados);

- **Cenário 8** - Um aplicativo malicioso (desenvolvido por um adversário para fins prejudiciais) pode obter dados privados do usuário e do aplicativo, caso o aplicativo principal registre esses dados no *log* do sistema móvel Android;
- **Cenário 9** - Um aplicativo malicioso pode obter dados privados do usuário e do aplicativo em dispositivos *rooted*, caso o aplicativo armazene esses dados de forma insegura (não criptografados);
- **Cenário 10** - Um aplicativo malicioso pode obter dados privados do usuário e do aplicativo, caso o aplicativo principal armazene esses dados no dispositivo de armazenamento externo;
- **Cenário 11** - Um adversário de rede pode obter dados privados do usuário e do aplicativo, caso não seja utilizado um canal de comunicação seguro (*SSL/TLS*);
- **Cenário 12** - Uma estação maliciosa com acesso físico ao dispositivo pode obter dados privados do usuário e do aplicativo mesmo quando adotada a proteção *Certificate Pinning*, em um ambiente não confiável, por exemplo, em dispositivos *rooted*;

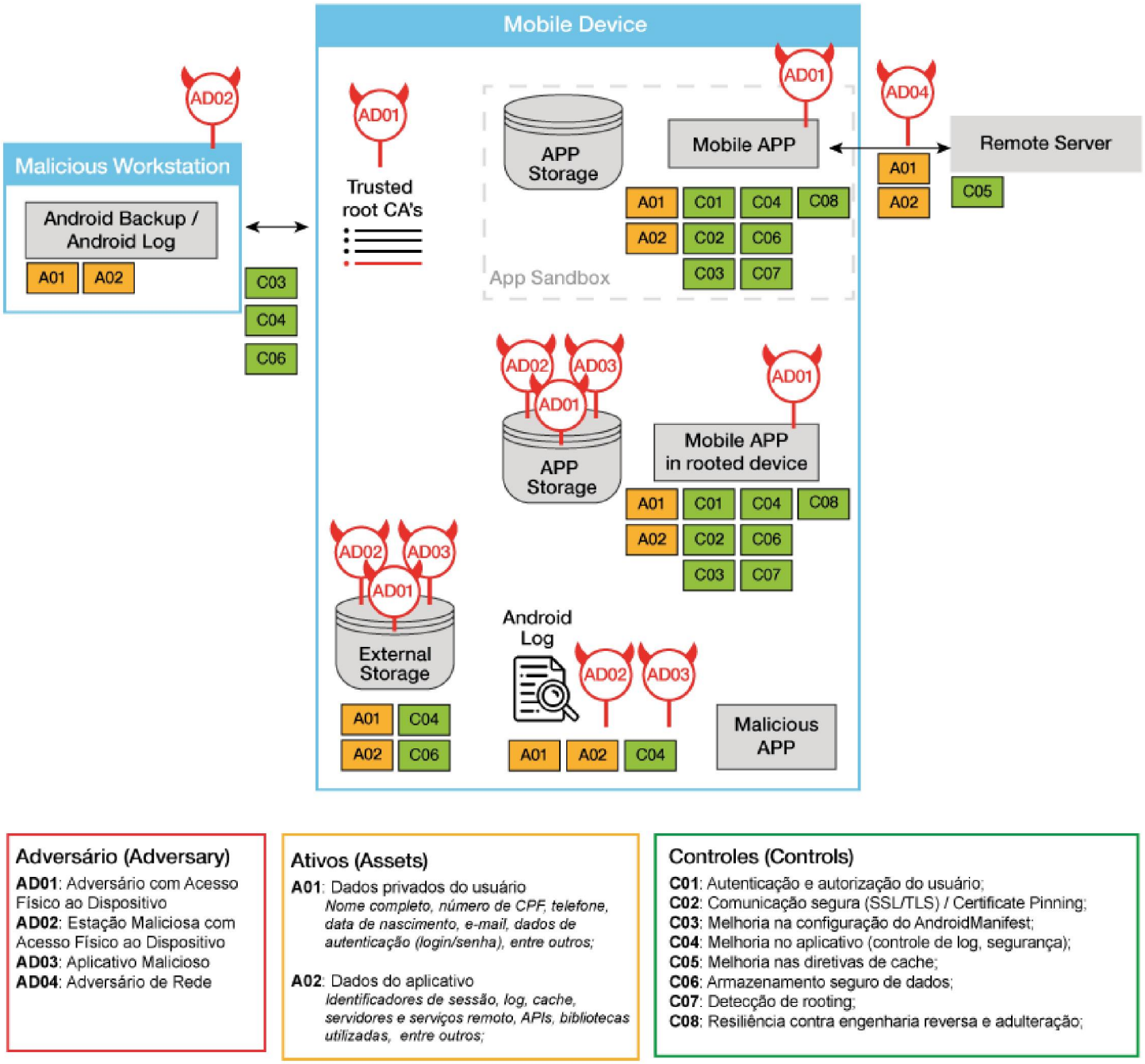


Figura 2.1: Diagrama do modelo de ameaça dos aplicativos analisados.

Tabela 2.3: Modelo de ameaça para os aplicativos analisados.

Cenário	Adversário	Ativo Alvo	Superfície de Ataque	Dispositivo Rooted	Risco (OWASP)	Mecanismo de Controle
Cenário 01	AD01: Adversário com Acesso Físico ao Dispositivo	A01: Dados privados do usuário	Aplicativo	Não	M4: Autenticação Insegura	C01: Autenticação e autorização do usuário
Cenário 02	AD01: Adversário com Acesso Físico ao Dispositivo	• A01: Dados privados do usuário • A02: Dados do aplicativo	Aplicativo / Dispositivo	Não	M7: Código de baixa qualidade	C02: Comunicação segura (SSL/-TLS) / Certificate Pinning
Cenário 03	AD01: Adversário com Acesso Físico ao Dispositivo	• A01: Dados privados do usuário • A02: Dados do aplicativo	Aplicativo	Não	• M8: Adulteração de código • M9: Engenharia Reversa	• C03: Melhoria na configuração do AndroidManifest; • C07: Detecção de rooting; • C08: Resiliência contra engenharia reversa e adulteração;
Cenário 04	AD01: Adversário com Acesso Físico ao Dispositivo	• A01: Dados privados do usuário • A02: Dados do aplicativo	Armazenamento Externo	Não	M7: Código de baixa qualidade	• C04: Melhoria no aplicativo (controle de log, segurança); • C06: Armazenamento seguro de dados;
Cenário 05	AD02: Estação Maliciosa com Acesso Físico ao Dispositivo	• A01: Dados privados do usuário • A02: Dados do aplicativo	Backup do aplicativo	Não	• M2: Armazenamento de dados inseguro; • M7: Código de baixa qualidade;	• C03: Melhoria na configuração do AndroidManifest; • C04: Melhoria no aplicativo (controle de log, segurança); • C06: Armazenamento seguro de dados;
Cenário 06	AD02: Estação Maliciosa com Acesso Físico ao Dispositivo	• A01: Dados privados do usuário • A02: Dados do aplicativo	Log do Android	Não	M7: Código de baixa qualidade	C04: Melhoria no aplicativo (controle de log, segurança)

Cenário	Adversário	Ativo Alvo	Superfície de Ataque	Dispositivo Rooted	Risco (OWASP)	Mecanismo de Controle
Cenário 07	AD02: Estação Maliciosa com Acesso Físico ao Dispositivo	• A01: Dados privados do usuário • A02: Dados do aplicativo	Aplicativo	Sim	• M2: Armazenamento de dados inseguro; • M7: Código de baixa qualidade;	• C04: Melhoria no aplicativo (controle de log, segurança); • C05: Melhoria nas diretivas de cache; • C06: Armazenamento seguro de dados; • C07: Detecção de rooting;
Cenário 08	AD03: Aplicativo Malicioso	• A01: Dados privados do usuário • A02: Dados do aplicativo	Log do Android	Não	M7: Código de baixa qualidade	C04: Aprimoramento do aplicativo (controle de log, segurança)
Cenário 09	AD03: Aplicativo Malicioso	• A01: Dados privados do usuário • A02: Dados do aplicativo	Aplicativo	Sim	• M2: Armazenamento de dados inseguro; • M7: Código de baixa qualidade;	• C04: Melhoria no aplicativo (controle de log, segurança); • C05: Melhoria nas diretivas de cache; • C06: Armazenamento seguro de dados; • C07: Detecção de rooting;
Cenário 10	AD03: Aplicativo Malicioso	• A01: Dados privados do usuário • A02: Dados do aplicativo	Armazenamento Externo	Não	M7: Código de baixa qualidade	• C04: Melhoria no aplicativo (controle de log, segurança); • C06: Armazenamento seguro de dados;
Cenário 11	AD04: Adversário de Rede	• A01: Dados privados do usuário • A02: Dados do aplicativo	Tráfego de rede	Não	M3: Comunicação Insegura	C02: Comunicação segura (SSL/-TLS) / Certificate Pinning
Cenário 12	AD02: Estação Maliciosa com Acesso Físico ao Dispositivo	• A01: Dados privados do usuário • A02: Dados do aplicativo	Aplicativo	Sim	• M3: Comunicação Insegura • M7: Código de baixa qualidade	• C02: Comunicação segura (SSL/TLS) / Certificate Pinning; • C04: Melhoria no aplicativo (controle de log, segurança); • C07: Detecção de rooting;

Importante constar que este estudo não aborda a totalidade de ameaças inerentes aos dispositivos móveis, pois seria necessária uma abordagem mais ampla sobre o ecossistema móvel, considerando aspectos como hardware, firmware, sistema operacional, tecnologias de comunicação (3G/4G/5G, Bluetooth, NFC, . . .), entre outros. Uma visão mais abrangente sobre as ameaças aos dispositivos móveis é apresentada no documento "*Assessing Threats to Mobile Devices & Infrastructure: The Mobile Threat Catalogue*", produzido pelo National Institute of Standards and Technology (NIST) (Franklin et al., 2016) e no documento "*Study on Mobile Device Security*", elaborado pelo U.S. Department of Homeland Security - DHS (2017).

Pode-se ainda observar que alguns cenários de ataque, ameaças e mecanismos de controle para aplicativos móveis não estão registrados nesta pesquisa. Todavia, destaca-se que o propósito deste estudo não é esgotar a análise de ameaças a aplicativos móveis, mas introduzir uma discussão relevante e suficiente para evidenciar o nível de segurança dos aplicativos do governo brasileiro. Tarandach e Coles (2020) alertam que o modelo de ameaças deve ser um documento vivo, em constante evolução.

2.7 ANÁLISE DE SEGURANÇA DE APLICATIVOS MÓVEIS

Para este estudo é importante compreender alguns conceitos e terminologias relacionadas à análise de segurança de aplicativo móvel. No decorrer deste estudo será utilizada a expressão "análise de segurança de aplicativo móvel" como referência para avaliação de segurança de aplicativo móvel por meio de análise estática e dinâmica. Conforme citado por Mueller et al. (2020), no documento "OWASP Mobile Security Testing Guide", essa expressão se aproxima a outros termos utilizados pela área de segurança, como "teste de penetração de aplicativos móveis" e "teste de segurança de aplicativos móveis", tratando-se do mesmo assunto. Desta forma, os termos "teste" e "análise" serão utilizados neste estudo com o mesmo sentido.

A segurança de aplicativos móveis engloba diferentes aspectos: a segurança dos próprios aplicativos móveis (plataforma Android e iOS), a segurança das APIs utilizadas e a segurança dos servidores remotos. Importante constar que este estudo tem como enfoque a avaliação da segurança dos aplicativos móveis do governo brasileiro para a plataforma Android e também da sua comunicação com servidores remotos. Não está incluso no escopo desta pesquisa a análise da segurança dos servidores que armazenam ou processam dados dos aplicativos.

Há diferentes formas de realizar testes em aplicativos móveis. Mueller et al. (2020) apresenta as seguintes formas:

- **Teste caixa-preta** - é conduzido sem que o testador tenha qualquer informação sobre o aplicativo que está sendo testado. Esse processo às vezes é chamado de "teste de conhecimento zero". O objetivo principal desse teste é permitir que o testador se comporte como um adversário real.

- **Teste caixa-branca** - é o oposto do teste caixa-preta, no sentido de que o testador tem total conhecimento do aplicativo. Às vezes é chamado de "teste de conhecimento total".

O conhecimento pode incluir código-fonte, documentação e diagramas, permitindo que o testador construa casos de teste mais sofisticados e granulares.

- **Teste caixa-cinza** - é todo o teste que se enquadra entre os dois tipos de teste anteriores. Algumas informações são fornecidas ao testador e outras devem ser descobertas.

Neste estudo será realizado o teste no modo caixa-preta, simulando o comportamento de um possível adversário. Porém, eventualmente, o teste pode ser semelhante ao teste caixa-cinza, em decorrência da descompilação do aplicativo estudado para a análise de seus artefatos internos. No entanto, vale destacar que a descompilação gera um código-fonte aproximado, não tratando-se do código-fonte original do aplicativo, por isso, difere-se do teste caixa-branca.

O teste da segurança de aplicativos pode ainda ser realizado a partir da abordagem da análise estática (manual ou automatizada) e da análise dinâmica. Tais abordagens podem ser definidas da seguinte forma:

- **Análise estática manual** - é o processo de revisão manual do código-fonte do aplicativo (original ou aproximado, decorrente de uma descompilação). A revisão manual pode ser lenta, tediosa e complexa, especialmente se houver o uso de muitas APIs de terceiros e se forem utilizadas técnicas de ofuscação de código.

- **Análise estática automatizada** - ferramentas de análise automatizadas podem ser usadas para acelerar o processo de detecção de vulnerabilidades em aplicativos. Essas ferramentas geralmente usam abordagens baseadas em um conjunto predefinido de regras ou práticas recomendadas e, em seguida, normalmente exibem uma lista de descobertas ou avisos para todas as violações detectadas.

- **Análise dinâmica** - é a avaliação de um aplicativo por meio de sua execução e observação do seu comportamento. É comumente utilizada para verificar dados em trânsito e problemas de configuração no servidor.

Há diversas ferramentas de análise automatizada, por exemplo, MobSF[5] (Dalziel e Abraham, 2016) permite a realização automatizada de teste de penetração, análise de malware e análise de segurança, através de análise estática e dinâmica. QARK[6] (Dalvi e Trummer, 2015) também é uma ferramenta conhecida para encontrar vulnerabilidades de segurança comuns em aplicativos Android. AndroBugs[7] (Lin, 2015) é outra ferramenta que promete auxiliar desenvolvedores a encontrar possíveis vulnerabilidades de segurança em aplicativos Android.

[5] https://github.com/MobSF/Mobile-Security-Framework-MobSF
[6] https://github.com/linkedin/qark
[7] https://github.com/AndroBugs/AndroBugs_Framework

Embora as ferramentas de análise automatizada incorporem muitas informações sobre as regras e a semântica necessárias para analisar aplicativos móveis, elas podem produzir muitos falsos positivos, exigindo que um profissional de segurança revise os resultados. Croft et al. (2021) avaliaram o desempenho de várias ferramentas comuns de análise estática de segurança de aplicações e relatam a ocorrência de falsos positivos nas ferramentas. Recentemente, a ferramenta COVIDGUARDIAN[8] propôs uma solução para reduzir o número de falsos positivos durante a análise estática automatizada (Sun et al., 2021), e será discutida em mais detalhes na Seção 2.8.

No entanto, devido a deficiências nessas ferramentas (ou seja, altas taxas de falsos positivos) e a necessidade de identificar exatamente quais dados sensíveis estão vulneráveis, este estudo optou por não fazer o uso de ferramentas automatizadas de análise de vulnerabilidades.

Neste estudo foi utilizada uma combinação entre a análise estática (manual e automatizada) e a análise dinâmica. Para a análise estática automatizada foram desenvolvidos pelo próprio pesquisador *scripts* de automatização de algumas atividades recorrentes. A inspeção manual foi utilizada como forma complementar à análise automatizada. A análise dinâmica foi empregada principalmente para observar a comunicação entre os aplicativos móveis e servidores remotos. Detalhes quanto à aplicação dessas abordagens de análise serão discutidas em mais detalhes no Capítulo 3.

2.8 TRABALHOS RELACIONADOS

O aumento no número de ataques a dispositivos móveis acompanhou o crescimento no uso desses equipamentos. Enquanto os desenvolvedores procuram aprimorar os mecanismos de segurança dos aplicativos e das plataformas móveis, os adversários buscam continuamente encontrar novas maneiras de comprometer esses mecanismos e obter dados pessoais dos usuários. Portanto, a segurança de aplicativos móveis é uma área de natureza dinâmica e emergente. Várias pesquisas cobrem o assunto de análise de segurança e vulnerabilidades de aplicativos Android sob perspectivas variadas e com foco em determinados contextos, por exemplo, bancário. Nesta seção serão apresentados alguns trabalhos importantes relacionados a este estudo.

Negi et al. (2021) apresentam uma revisão sobre a arquitetura do Android, a fim de entender cada um dos seus componentes e como eles estão organizados, e a estrutura de um aplicativo, com as principais pastas e arquivos que compõem um aplicativo. Na sequência o artigo apresenta um modelo de ameaças no qual os ataques são analisados de acordo com as camadas nas quais eles atuam, podendo ser camada de kernel, camada de middleware e camada de aplicação. Por fim, são realizados estudos de caso para ilustrar a detecção de aplicativos de *malware*, utilizando a ferramenta MobSF para extrair dados dos aplicativos e algoritmos de aprendizado de máquina para classificação desses aplicativos.

[8] https://covid-guardian.github.io/

Bergadano et al. (2020) propõe uma nova ferramenta para análise de segurança de aplicativos móveis. A ferramenta é baseada em uma combinação de análise estática e dinâmica e adota o OWASP Mobile Top Ten como uma diretriz de vulnerabilidades. Para aplicativos Android, os módulos se concentram na análise de áreas relacionadas com armazenamento de dados e comunicação de rede, além do arquivo de manifesto. Realizou-se ainda a avaliação de outras ferramentas de análise estática e dinâmica. O estudo também analisou a segurança de 105 aplicativos móveis coletados na Google Play, nas áreas de finanças, criptomoedas, compras, viagens, comunicação e redes sociais. Segundo os autores, essa ferramenta diferencia-se de outras (por exemplo, MobSF) por automatizar algumas atividades secundárias, como já realizar o backup de dados do aplicativo, caso essa funcionalidade seja permitida no arquivo de manifesto do Android. No entanto, a análise por conteúdo sensível no backup do aplicativo continua manual. A pesquisa identificou um conjunto de vulnerabilidades nos aplicativos e também sugeriu aumentar a consciência de segurança não apenas para desenvolvedores, mas também para usuários.

No estudo de Sun et al. (2021), foi conduzida uma avaliação abrangente de segurança e privacidade de 40 aplicativos de rastreamento de contato com pessoas contaminadas durante a pandemia de Covid-19. O estudo também desenvolveu uma ferramenta de avaliação automatizada de segurança e privacidade, batizada de COVIDGUARDIAN. Segundo os autores, a ferramenta apresentou resultado superior às ferramentas mais utilizadas (MobSF, Androbugs, FlowDroid e QARK) de mesmo propósito. O diferencial dessa ferramenta é que o COVIDGUARDIAN utiliza análise estática e dinâmica, bem como um banco de dados de palavras-chave utilizando tecnologia de processamento de linguagem natural, para identificar pontos fracos de segurança e vazamento de informações pessoais em aplicativos. O estudo ainda realizou uma pesquisa envolvendo 373 participantes, para investigar as preocupações e requisitos do usuário quanto aos aplicativos de rastreamento de contato Covid-19. Os resultados indicam que a precisão do rastreamento e os riscos potenciais à privacidade são as duas principais preocupações. A pesquisa confirmou que nenhum aplicativo analisado protegeu a segurança e a privacidade dos usuários contra todas as ameaças potenciais. Em outro estudo, Kohli e Mohaghegh (2020) testaram quatro aplicativos de rastreamento de contato com pessoas contaminadas com a Covid-19 utilizando MobSF e Drozer para verificar vulnerabilidades de segurança. Os aplicativos testados apresentaram uma pontuação de segurança muito baixa, demonstrando não serem seguros.

Botacin et al. (2019) analisaram a evolução do serviço bancário no Brasil, a transformação de softwares desktop para aplicativos móveis nesse setor e também o aperfeiçoamento das técnicas utilizadas por adversários. Na sequência, o estudo realizou uma análise detalhada da segurança de seis aplicativos bancários brasileiros, disponíveis na loja de aplicativos Android, e identificou que os desenvolvedores ainda não seguem as práticas de desenvolvimento seguro, fazendo com que os aplicativos bancários vazem dados confidenciais do usuário. Por fim, foram apresentados novos ataques que podem ameaçar os usuários em um curto prazo, em particular, um ataque contra um mecanismo de transação baseado em Whatsapp, implementado por alguns bancos.

Ainda no segmento de aplicativos bancários, Osho et al. (2019) fazem uma investigação de doze aplicativos populares na Nigéria, a fim de determinar se: i) os backups gerados pelo sistema operacional móvel não salvam dados confidenciais; ii) o aplicativo remove dados confidenciais em segundo plano; iii) os dados sensíveis não são mantidos por mais tempo do que o necessário na memória; iv) as políticas de segurança de acesso mínimo ao dispositivo são aplicadas; v) os usuários são instruídos pelo aplicativo sobre o tipo dados pessoais processados. O estudo utilizou a ferramenta UFED[9], da empresa Cellebrite, para fazer a aquisição física da memória do dispositivo e para análise dos dados foi utilizada a ferramenta Forensic Recovery Evidence Device[10] (FRED). O estudo aplica uma visão forense à análise dos aplicativos e não faz o uso de ferramentas de análise estática ou análise dinâmica, voltadas para a segurança de aplicativos móveis. O estudo revelou que, embora nenhum dos aplicativos salvasse dados confidenciais no backup gerado, todos, exceto um, mantinham dados de valor confidencial na memória do dispositivo de teste e não impunham nenhuma política de segurança de acesso ao dispositivo. Além disso, nenhum dos aplicativos removeu dados confidenciais em segundo plano.

Lero et al. (2019) examinaram a segurança de aplicativos de criptomoeda comumente utilizados, buscando vulnerabilidades comuns descritas pelo OWASP Mobile Top Ten 2016. O estudo analisou 48 aplicativos de criptomoedas e 10 aplicativos bancários tradicionais. O objetivo é comparar o estado de segurança de aplicativos de criptomoedas e aplicativos bancários. Os aplicativos foram examinados utilizando a ferramenta de análise estática automatizada DroidSafe (Gordon et al., 2015). O estudo também explora as limitações da análise de código estático e examina a validade do teste estático para avaliação de segurança de aplicativos móveis. O estudo relata que o problema mais comum dos aplicativos é a criptografia insuficiente, seguida pelo armazenamento inseguro de dados.

Phumkaew e Visoottiviseth (2018) conduziram uma análise de segurança de três aplicativos móveis de hospital e cinco aplicativos móveis de estoque e comércio na Tailândia. As descobertas foram mapeadas segundo o OWASP Mobile Top Ten 2016. A pesquisa foi conduzida através da análise estática e dinâmica de cada aplicativo. O estudo não fez uso de nenhuma ferramenta de análise automatizada de segurança. O estudo identificou que há risco de exposição e vazamento de dados para terceiros não autorizados por esses aplicativos. É acrescentado ainda que os usuários devem estar atentos a algumas medidas de segurança, como não se conectar a uma rede pública insegura ou baixar e instalar aplicativos de sites não oficiais.

Neto (2020), em sua tese de doutorado, examina como órgãos públicos têm adotado aplicativos móveis para aprimorar sua interação com diferentes atores da sociedade (empresas, servidores públicos, população de um modo gera, etc.). O estudo também investiga os diferentes tipos de práticas e modelos de desenvolvimento, bem como a opinião dos usuários em relação aos aplicativos mapeados. A amostra desta pesquisa é composta por 203 aplicativos mapeados

[9] https://cellebrite.com/pt/cellebrite-ufed-pt/

[10] https://www.dataexpert.eu/products/forensic-hardware-digital-intelligence/fred-workstation/

a partir da página de desenvolvedor de 43 órgãos do setor público brasileiro no Google Play. Vale notar que durante este estudo os aplicativos ainda não estava centralizados em uma conta única do Governo Federal, conforme estabelece a Portaria nº 39, de 09/07/2019, do Ministério da Economia. O estudo apontou que Embrapa, SERPRO e DATASUS eram responsáveis por parte significativa dos aplicativos móveis governamentais e que há diferentes modelos de desenvolvimento de aplicativos, sendo os principais: desenvolvimento interno, desenvolvimento por terceirizado, desenvolvimento por empresa pública e desenvolvimento por concurso. Neto, no entanto, não analisa os aplicativos governamentais sob um panorama técnico, principalmente com relação aos aspectos de vulnerabilidades de segurança e privacidade dos dados, sendo um importante diferencial desta pesquisa.

Um guia essencial sobre a análise de segurança de aplicativos móveis é o "OWASP Mobile Security Testing Guide" (Mueller et al., 2020). Esse documento é um manual abrangente para teste de segurança de aplicativo móvel e engenharia reversa, utilizado amplamente por avaliadores de segurança móvel Android e iOS. Ele cobre processos, técnicas e ferramentas usadas durante um teste de segurança de aplicativo móvel.

Outro material relevante sobre o assunto é o livro "Mobile Application Penetration Testing" (Velu, 2016). Ele fornece uma ótima referência sobre ataques a aplicativos móveis e maneiras de combatê-los. Esse livro fornece ainda um guia passo a passo que vai desde a configuração de um ambiente de teste até a realização dos testes de penetração em aplicativos móveis. Ele aborda detalhes das arquiteturas Android e iOS e apresenta algumas ferramentas para a realização dos testes de penetração.

Diante da análise dos estudos anteriores, foi possível observar que o OWASP Mobile To Ten 2016 é o guia de referência para identificar os principais riscos de segurança enfrentados por aplicativos móveis. Verificou-se que os estudos são bastante contextualizados, analisando aplicativos de categorias específicas, em especial aqueles que lidam com dados sensíveis, como dados financeiros e de saúde. No entanto, não se tem conhecimento de nenhuma pesquisa que investigue a segurança e a privacidade de usuários de aplicativos móveis de governo. A maioria dos estudos fazem uso de ferramentas de automatização da análise estática, no entanto, sempre acompanhada da análise manual, uma vez que é percebida as limitações de uma análise de segurança baseada apenas em ferramentas automatizadas.

Esta pesquisa, no entanto, se destaca pela análise aprofundada de aplicativos móveis do governo brasileiro. Como em outros trabalhos, não são registradas fragilidades nos aplicativos por meio de ferramentas de teste automatizado, como visto, bastante suscetíveis a resultados falsos positivos. As principais vulnerabilidades dos aplicativos móveis do governo brasileiro são apresentadas de forma detalhada e destacados quais dados dos usuários e dos aplicativos podem ser comprometidos. Diante dos resultados da pesquisa e das recomendações à Administração Pública e ao cidadão, este estudo contribui para a construção de um país onde os dados pessoais são devidamente protegidos e a privacidade do cidadão é respeitada.

Este Capítulo fez uma revisão da fundamentação teórica necessária ao desenvolvimento da pesquisa. Foi abordada a utilização da tecnologia móvel pelo setor público, em especial pelo governo brasileiro. Foram realizadas considerações sobre a Lei Geral de Proteção de Dados Pessoais e apresentadas as vulnerabilidades e os comportamentos inseguros dos usuários, que podem afetar a segurança de aplicativos móveis, em conjunto com um diagrama de modelo de ameaças. Foram abordados ainda conceitos relacionados à análise de segurança de aplicativos e, por fim, apresentados alguns trabalhos relacionados.

No próximo Capítulo serão apresentados os parâmetros utilizados para seleção dos aplicativos móveis do governo brasileiro, os critérios de segurança e privacidade estabelecidos, o método de análise e as ferramentas utilizadas nesta pesquisa.

3 MÉTODO

Neste Capítulo é apresentado o método utilizado para avaliar a segurança e a privacidade dos aplicativos móveis do governo brasileiro. Os aplicativos móveis selecionados são apresentados na Seção 3.1, enquanto os critérios de segurança e privacidade são debatidos na Seção 3.2. Na sequência, são apresentados o ambiente de teste (Seção 3.3), as ferramentas utilizadas (Seção 3.4) e, por fim, o método de análise (Seção 3.5).

3.1 SELEÇÃO DOS APLICATIVOS DO GOVERNO BRASILEIRO

Os aplicativos móveis a serem avaliados quanto à segurança e à privacidade foram selecionados de acordo com quatro critérios: I. **aplicativos oficiais**, ou seja, apenas aqueles presentes na conta oficial do governo brasileiro; II. **destinados à plataforma Android**, em decorrência de ser o sistema móvel utilizado por 86,9% dos brasileiros, segundo dados da Statcounter (2020); III. **voltados ao cidadão**, isto é, aqueles acessíveis a qualquer pessoa que queira utilizar um serviço do governo por meio de aplicativo; IV. **com mais de 100 (cem) mil downloads**, de modo a considerar aqueles que possuem um uso significativo.

Deste modo, foram selecionados 30 aplicativos, que totalizam mais de 93,5 milhões de downloads, os quais representam 95,8% dos downloads de aplicativos Android da loja oficial do governo brasileiro[1], conforme tabela 3.1. Os aplicativos são apresentados de forma anonimizada, no entanto, todos os detalhes de cada aplicativo encontram-se no Apêndice A, o qual será mantido em sigilo por um prazo definido, conforme esclarecido na Seção 1.4.

Tabela 3.1: Aplicativos móveis selecionados e número de downloads.

#	Aplicativo	Downloads	#	Aplicativo	Downloads
1	A01	+ 10 milhões	16	A16	+1 milhão
2	A02	+10 milhões	17	A17	+1 milhão
3	A03	+10 milhões	18	A18	+500 mil
4	A04	+10 milhões	19	A19	+500 mil
5	A05	+5 milhões	20	A20	+500 mil
6	A06	+10 milhões	21	A21	+100 mil
7	A07	+10 milhões	22	A22	+100 mil
8	A08	+5 milhões	23	A23	+100 mil
9	A09	+5 milhões	24	A24	+100 mil
10	A10	+5 milhões	25	A25	+100 mil
11	A11	+5 milhões	26	A26	+100 mil
12	A12	+1 milhão	27	A27	+100 mil
13	A13	+1 milhão	28	A28	+100 mil
14	A14	+1 milhão	29	A29	+100 mil
15	A15	+1 milhão	30	A30	+100 mil

[1] https://play.google.com/store/apps/dev?id=5829287075355252046

3.2 CRITÉRIOS AVALIADOS DE SEGURANÇA E PRIVACIDADE

Conforme discutido previamente na Seção 2.7, a segurança de aplicativos móveis envolve diferentes aspectos: a segurança dos próprios aplicativos móveis, a segurança das APIs e a segurança dos servidores. Este estudo tem como foco a análise da segurança dos aplicativos e da comunicação destes com servidores remotos. Para tanto, os aplicativos do governo brasileiro serão examinados considerando os principais tipos de riscos enfrentados por aplicativos móveis, segundo o OWASP Mobile Top Ten 2016.

Este estudo elencou quatorze critérios mais impactantes, que foram separados em cinco categorias: I. Arquivo de manifesto; II. Armazenamento de dados; III. Transmissão de dados; IV. Permissões perigosas; V. Outros riscos. A Tabela 3.2 apresenta os critérios selecionados, a categoria na qual se enquadram e o tipo de vulnerabilidade, segundo o OWASP, discutido anteriormente na Seção 2.4. Caso um aplicativo não atenda esse conjunto de critérios, é altamente provável que a segurança e a privacidade dos dados do cidadão estejam vulneráveis.

3.2.1 Arquivo de Manifesto

Atributo AllowBackup

Todo projeto de aplicativo tem um arquivo `AndroidManifest.xml` que descreve informações essenciais sobre o aplicativo para as ferramentas de compilação, para o sistema operacional Android e para a loja de aplicativos da Google (Google Play). Neste arquivo de manifesto o atributo `allowBackup` é responsável por estabelecer as configurações de backup e restauração do aplicativo.

Se o valor para este atributo for *true* (*verdadeiro*), será possível fazer o backup dos dados do aplicativo, inclusive de dados sensíveis armazenados sem a devida proteção. Deste modo, um usuário malicioso com acesso físico ao dispositivo pode facilmente fazer o backup dos dados armazenados pelo aplicativo.

Para evitar o backup de dados, o aplicativo deve definir no arquivo de manifesto o atributo `allowBackup` como *false* (*falso*). Deve-se atentar que quando esse atributo não estiver definido no arquivo de manifesto, a configuração `allowBackup` é *true* (*verdadeira*) por padrão. Portanto, é aconselhado que as definições de backup do aplicativo sejam definidas explicitamente.

Atributo Debuggable

O Android fornece o atributo `debuggable` para especificar se um aplicativo pode ser depurável ou não depurável. Este atributo deve estar sempre definido como *false* (*falso*), para a versão de produção do aplicativo. O atributo `debuggable` configurado como *true* (*verdadeiro*) permitirá, por exemplo, que um adversário adultere o comportamento do aplicativo em tempo de execução, contornando mecanismos de proteção, como *SSL Pinning*, permitindo a interceptação do tráfego de dados, inclusive em canais seguros (HTTPS).

Tabela 3.2: Critérios avaliados de segurança e privacidade.

Categoria	**Critério avaliado**	**Risco OWASP**
Arquivo de Manifesto	AM1: O atributo `allowBackup` está configurado de forma apropriada, não permitindo o backup de dados sensíveis	M2
	AM2: O atributo `debuggable` está configurado de forma apropriada para um aplicativo em versão de produção (não *debuggable*).	M7
	AM3: O atributo `usesCleartextTraffic` está configurado de forma apropriada, não permitindo que o aplicativo e bibliotecas de terceiros trafeguem dados de forma insegura	M3
Armazenamento de Dados	AD1: O aplicativo armazena dados sensíveis localmente de forma segura	M2
	AD2: O aplicativo não armazena dados sensíveis em arquivos de cache	M2
	AD3: O aplicativo não registra dados sensíveis em arquivos de *log* ou no *log* do sistema operacional	M2
	AD4: O aplicativo adota proteção contra a captura de dados sensíveis em auto-screenshots, quando o aplicativo é colocado em segundo plano	M2
Transmissão de Dados	TD1: O aplicativo trafega dados em um canal de comunicação de rede seguro (criptografado)	M3
	TD2: O aplicativo adota medida de proteção da comunicação de rede por *SSL Pinning*	M3
Permissões Perigosas	PP: O aplicativo não solicita permissões perigosas além do mínimo necessário	M1
Outros Riscos	OR1: O aplicativo não compartilha dados com terceiros (ex. *Google Firebase*)	M2
	OR2: O aplicativo não utiliza rastreadores (*trackers*) que podem comprometer a privacidade do usuário	M2
	OR3: O aplicativo adota medidas para detectar e responder adequadamente a um dispositivo *rooted*	M8
	OR4: O aplicativo exige a autenticação do usuário a cada novo acesso ao aplicativo (não adota autenticação persistente)	M4

Atributo usesCleartextTraffic

O Android fornece o atributo `usesCleartextTraffic` para determinar se o aplicativo permite o tráfego de rede em texto simples (não criptografado). Este atributo deve estar sempre configurado com o valor *false* (*falso*), para que os componentes da plataforma recusem o tráfego em texto simples, inclusive de bibliotecas de terceiros. Se o valor do atributo `usesCleartextTraffic` for *true* (*verdadeiro*), um adversário de rede poderá inspecionar os dados transmitidos em texto simples (não criptografados), comprometendo a privacidade do usuário.

Deve-se atentar que quando esse atributo não estiver definido no arquivo de manifesto, a configuração `usesCleartextTraffic` é considerada *true* (*verdadeira*) por padrão, em aplicativos direcionados ao Android 8.1 (API27) e versões anteriores, permitindo o tráfego de dados de forma insegura (não criptografados). Portanto, é aconselhada a definição deste atributo de forma explícita.

3.2.2 Armazenamento de Dados

Armazenamento seguro de dados sensíveis localmente

O armazenamento de dados é essencial para muitas aplicações. Os aplicativos podem armazenar dados do usuário, dados de autenticação, dados de localização e diversos outros dados sensíveis. O Android fornece vários métodos para armazenamento de dados, dependendo das necessidades do usuário, do desenvolvedor e do aplicativo. Algumas das técnicas mais usadas na plataforma Android são: arquivos *Shared Preferences*, banco de dados SQLite e Firebase, arquivos XML e arquivos de texto. No entanto, é recomendado que os aplicativos armazenem o mínimo de informações sensíveis localmente (Mueller et al., 2020). Quando for imprescindível o armazenamento local, é fundamental que este armazenamento seja feito de forma segura, ou seja, criptografado.

Deve-se considerar que um adversário com acesso físico ao equipamento ou um aplicativo malicioso (*malware*) pode explorar vulnerabilidades no aplicativo ou no dispositivo para obter dados sensíveis do usuário armazenados de forma insegura.

Armazenamento inadequado de dados sensíveis em arquivos de cache

Os aplicativos podem armazenar dados para fins de *cache*. *Cache* é um recurso utilizado para melhorar o desempenho de um aplicativo, de modo que as informações requisitadas anteriormente não precisem ser solicitadas novamente. Se um serviço remoto retornar dados sensíveis do usuário (como número de CPF, endereço e outros dados pessoais), estes dados podem ser armazenados para fins de *cache*.

Deste modo, desenvolvedores devem adotar mecanismos para evitar que arquivos de *cache* armazenem de forma inapropriada dados sensíveis do usuário.

Armazenamento inadequado de dados sensíveis em arquivos de log ou no log do sistema

Existem muitos motivos legítimos para criar arquivos de *log* em um dispositivo móvel, como para rastrear travamentos, erros e estatísticas de uso do aplicativo. Os arquivos de *log* podem ser armazenados localmente, quando o aplicativo está "*offline*", e posteriormente enviados para um servidor remoto, quando o aplicativo está "*online*". No entanto, o registro em *log* de dados sensíveis pode expor dados do usuário a adversários ou aplicativos maliciosos, violando a privacidade do usuário (Mueller et al., 2020).

Sendo assim, é primordial que seja garantido que dados potencialmente sensíveis não sejam registrados em arquivos de *log* do aplicativo e no *log* do sistema móvel.

Armazenamento inadequado de dados sensíveis em auto-screenshots

Para fornecer uma experiência esteticamente agradável na transição entre aplicativos, o Android utiliza um recurso de captura automática de tela. Este recurso captura e armazena a tela do dispositivo, sempre que um aplicativo é colocado em segundo plano. Deste modo, a privacidade do usuário pode ser comprometida, se a captura de tela ocorrer enquanto o aplicativo exibe dados sensíveis do usuário.

Considerando que as capturas de tela são armazenadas localmente no dispositivo, um adversário com acesso físico ao dispositivo ou um aplicativo malicioso poderia obter estas capturas de tela contendo dados sensíveis, principalmente em dispositivos *rooted*. O *rooting* de dispositivos é um comportamento inseguro que deve ser previsto pelos desenvolvedores de aplicativos, conforme abordado na Seção 2.5.

3.2.3 Transmissão de Dados

Utilização de canal seguro

Os aplicativos móveis comumente trocam dados com um servidor remoto, no modelo cliente-servidor. No caminho entre o dispositivo móvel e o servidor remoto, os dados trafegam pela rede do usuário, pela rede da operadora do usuário e pela Internet. Deste modo, um adversário poderia inspecionar os dados trafegados em cada um dos pontos deste caminho. Porém, é mais fácil para o adversário monitorar o tráfego em um ponto de acesso público, como uma cafeteria, do que monitorar o tráfego de uma operadora de acesso à Internet.

Considerando que os usuários adotam comportamentos inseguros, transmitindo dados sensíveis através de redes Wi-Fi públicas, conforme discutido na Seção 2.5, para garantir segurança de ponta a ponta nos canais de comunicação, os desenvolvedores devem utilizar protocolos de comunicação segura, tal como SSL/TLS. Transport Layer Security (TLS) é o sucessor do Secure Sockets Layer (SSL), todavia, é comum se referir a essas tecnologias apenas como "SSL" ou "SSL/TLS". SSL/TLS é uma tecnologia de segurança para estabelecer um canal de comunicação criptografado entre um cliente e um servidor, garantindo que todos os dados transmitidos entre eles permaneçam privados.

Utilização de SSL Pinning

Importante destacar que a utilização apenas da tecnologia SSL/TLS pode não ser suficiente para garantir a privacidade dos dados trafegados, por exemplo, caso um adversário utilize a técnica MitM em conjunto com um certificado SSL/TLS mal-intencionado (CWE295). *Man in the Middle* (MitM), como o nome sugere, refere-se a uma técnica na qual um adversário insere-se no meio das comunicações entre aplicativo cliente e o servidor. Nesta posição é possível interceptar, ler e modificar o tráfego "de/para" os dois dispositivos, afetando a confidencialidade e a integridade dos dados.

Nesta técnica são utilizados ainda os conceitos de Certificado Digital e de Infraestrutura de Chaves Públicas, sendo instalado no dispositivo móvel cliente o certificado de uma autoridade certificadora (*Certification Authority - CA*) mal-intencionada, na qual o cliente passa a confiar. Deste modo, quando o cliente está se comunicando com o servidor remoto, na verdade, ele está se conectando com um adversário. Assim, o cliente acredita ter estabelecido uma conexão criptografada com o servidor, mas na realidade ambos (cliente e servidor) estão realmente se comunicando com um adversário, que utiliza um certificado digital assinado por uma Autoridade Certificadora na qual o dispositivo móvel passou a confiar e, desta forma, torna-se possível visualizar e modificar todos os dados trafegados, conforme Figura 3.1.

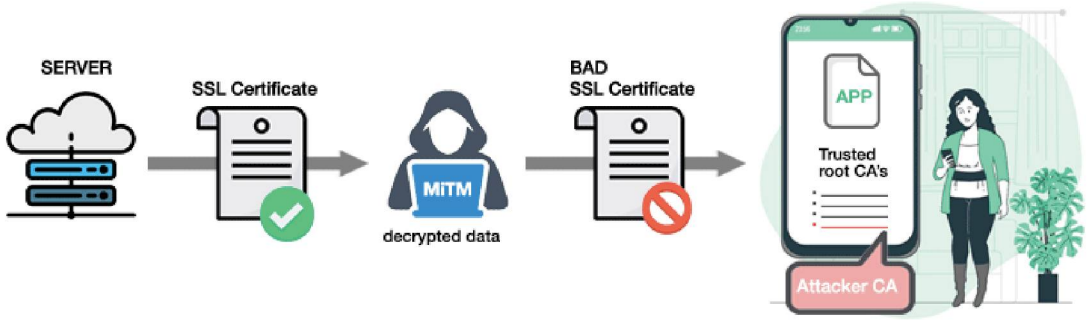


Figura 3.1: Ataque *Man in the Middle* (MitM) à comunicação SSL/TLS.

A estratégia conhecida como "*SSL Pinning*" é uma contramedida a este tipo de vulnerabilidade. Segundo Mueller et al. (2020), "*SSL Pinning*" é o processo de associar o servidor a um certificado X.509 específico ou uma chave pública em vez de o aplicativo aceitar qualquer certificado assinado por uma autoridade de certificação confiável. Depois de armazenar ("*pinning*") o certificado do servidor ou a chave pública, o aplicativo móvel se conectará somente com o servidor predefinido. Tal certificado poderá ser armazenado no próprio aplicativo ou recuperado remotamente do servidor. Limitar a confiança em um certificado específico reduz a superfície de ataque ao aplicativo. Caso não seja implementado "*SSL Pinning*", o aplicativo poderá confiar em um certificado mal-intencionado e permitir que ferramentas de proxy interceptem a comunicação de dados.

3.2.4 Permissões Perigosas

O sistema de permissões do Android é um mecanismo para garantir a segurança e a privacidade do usuário. Seu objetivo é ajudar o usuário a ter controle sobre quais dados ele compartilha com os aplicativos. As permissões também são um meio de limitar que os aplicativos acessem dados desnecessários (Android Developers, 2021). Porém, esse mecanismo depende que os desenvolvedores de aplicativos sigam um conjunto de práticas recomendadas. Muitos desenvolvedores, no entanto, tendem a solicitar permissões além do necessário, colocando em risco a privacidade dos usuários, por exemplo, solicitando permissões conhecidas por "*permissões perigosas*". Permissões perigosas são um tipo especial de permissões que dão acesso a dados restritos do usuário, incluindo informações potencialmente confidenciais, como dados de localização e dados de ligações. A lista de todas as permissões perigosas possíveis pode ser consultada na documentação oficial do Android[2].

3.2.5 Outros riscos

Compartilhamento de dados com terceiros

Muitos aplicativos incorporam serviços de terceiros para armazenamento remoto de dados. A exemplo, um dos serviços de nuvem mais utilizados é o *Firebase*, oferecido como parte integrante do *Google Cloud Platform*. Esse serviço é utilizado para armazenar e sincronizar dados em tempo real. Muitos desenvolvedores utilizam esses recursos com a justificativa de oferecer uma melhor experiência no aplicativo, todavia, seu uso pode trazer riscos para a segurança dos dados dos usuários.

Uma pesquisa da empresa de segurança cibernética *Check Point* descobriu que muitos aplicativos Android expuseram publicamente dados confidenciais de mais de 100 milhões de usuários por meio de serviços de terceiros mal configurados (Hazum et al., 2021). Os dados expostos incluem e-mails, senhas, informações de localização, fotos, identificadores de usuários, mensagens de bate-papo e muito mais.

Outro problema, é a falta de transparência dos aplicativos, não informando aos usuários que seus dados serão armazenados em serviços de terceiros e não esclarecendo quais os dados que serão coletados e armazenados.

Utilização de rastreadores

Segundo a Exodus Privacy (2021), uma organização sem fins lucrativos que tem o objetivo de ajudar pessoas a compreenderem melhor os problemas de rastreamento de aplicativos Android, um rastreador (*tracker*) é um software cuja função é coletar informações sobre quem usa o aplicativo, como usa ou sobre o dispositivo que está em uso. Um rastreador normalmente é distribuído pelas empresas na forma de um kit de ferramentas pronto para o uso dos desenvolvedores.

[2] `https://developer.android.com/reference/android/Manifest.permission`

Os rastreadores não têm a mesma função e podem apresentar diferentes níveis de invasão de privacidade:

- ***Crash reporters*** - esses rastreadores são especializados em relatar falhas em aplicativos. Em outros termos, seu objetivo é notificar os desenvolvedores de aplicativos de que o aplicativo encontrou um problema. Dessa forma, as informações coletadas no momento em que o aplicativo falhou permitirão que o desenvolvedor corrija o problema;

- ***Analytics*** - esses rastreadores têm como objetivo coletar informações sobre o uso do aplicativo e permitir que o desenvolvedor tenha um melhor conhecimento de seu público (por exemplo, as funcionalidades acessadas ou o tempo que o usuário permaneceu em determinada funcionalidade);

- ***Profiling*** - o objetivo desses rastreadores é reunir o máximo de informações possível sobre o usuário do aplicativo, para construir um perfil virtual. Para este efeito, o rastreador irá, por exemplo, focar no histórico de navegação, ou na lista de aplicativos instalados, e assim por diante;

- ***Identification*** - esses rastreadores são responsáveis por determinar sua identidade digital. Essa identidade pode se referir a uma identidade oficial ou a identificadores abstratos (pseudônimo, etc.). O objetivo será, por exemplo, ser capaz de correlacionar as atividades *online* e *offline* de um indivíduo;

- ***Ads*** - esses rastreadores têm como objetivo identificar o usuário do aplicativo para veicular anúncios direcionados. Isso só é possível e relevante se o usuário já tiver um perfil digital estabelecido. O objetivo do criador de tal rastreador é monetizar seu aplicativo, ou seja, ganhar dinheiro por meio de propaganda.

- ***Location*** - esses rastreadores são projetados para determinar a localização geográfica do dispositivo móvel. Para isso, este tipo de rastreador tira proveito de vários sensores: GPS, antenas de celular circundantes, redes Wi-Fi presentes na área, redes Bluetooth próximas ou mesmo sons específicos transmitidos por alto-falantes.

Detecção de dispositivo rooted

O objetivo da detecção de dispositivo *rooted* é assegurar que o aplicativo seja executado em um dispositivo seguro. Um dispositivo não *rooted* dificulta o uso de muitas ferramentas e técnicas de engenharia reversa utilizadas por adversários. Já um dispositivo *rooted* compromete os mecanismos de segurança do dispositivo e pode expor os dados do usuário a uma violação de privacidade (Casati e Visconti, 2018). Os desenvolvedores devem avaliar os impactos na segurança de seus aplicativos, caso os usuários utilizem dispositivos *rooted*.

Autenticação persistente

Autenticação é o procedimento no qual o usuário "desbloqueia" um aplicativo, normalmente, fornecendo uma senha ou uma característica biométrica, como a face ou uma impressão digital. Essa autenticação pode ainda ser em duas etapas, como um recurso adicional de segurança. É imprescindível que aplicativos que manipulam dados pessoais utilizem mecanismos adequados de segurança. No entanto, muitos desenvolvedores adotam esquemas de autenticação deficientes ou ausentes, permitindo que um adversário execute anonimamente uma funcionalidade em um aplicativo móvel e tenha acesso a dados sensíveis.

Segundo o *OWASP Mobile Top Ten 2016*, a utilização de autenticação persistente, habilitada por padrão, é um esquema de design de autenticação de aplicativo móvel inseguro. Neste caso, após a primeira autenticação do usuário, o aplicativo é mantido em um estado persistente de autenticação, não requerendo uma nova autenticação a cada acesso ao aplicativo. Esse esquema de autenticação pode tornar os dados do usuário vulneráveis, uma vez que qualquer pessoa com acesso ao dispositivo pode verificar aos dados pessoais do usuário no aplicativo, sem a necessidade de autenticação.

3.3 CONFIGURAÇÃO DO AMBIENTE DE TESTE

Na sequência serão apresentadas as configurações do ambiente utilizado para testar os aplicativos móveis do governo brasileiro.

3.3.1 Dispositivo *host*

O dispositivo *host* é o equipamento utilizado para instalação das ferramentas de apoio a este estudo. O dispositivo é um MacBook Pro (2011), sistema operacional MacOs High Sierra (v10.13.6) e com as ferramentas de apoio descritas na Seção 3.4.

3.3.2 Dispositivo móvel de teste

Os aplicativos a serem avaliados foram instalados em um dispositivo físico com o sistema móvel Android. O equipamento tinha a seguinte configuração: marca Motorola, modelo Moto E (XT1763), Android 7.1.1 (API 25). Foi realizado o *rooting* do dispositivo utilizando a ferramenta Magisk[3]. *Rooting* é o ato de modificar o sistema operacional móvel do dispositivo para obter privilégios de superusuário.

[3] `https://magiskmanager.com`

3.3.3 Configuração de Rede

Para inspecionar o tráfego de dados entre o aplicativo móvel e servidores remotos, isto é, requisições/respostas HTTP e HTTPS, foi configurado um *proxy* de interceptação no dispositivo *host* utilizando a ferramenta "Mitmproxy", descrita em mais detalhes na seção seguinte.

O dispositivo móvel precisou ter sua configuração de rede alterada manualmente para utilizar o servidor *proxy*. Para permitir a interceptação do tráfego HTTPS foi necessário instalar no dispositivo móvel um certificado de Autoridade Certificadora (*Certification Authority - CA*), gerado pela ferramenta "Mitmproxy". Os procedimentos de geração e instalação do certificado digital no dispositivo móvel são detalhados na documentação da própria ferramenta[4].

A comunicação de rede entre o dispositivo móvel e o dispositivo *host* (o qual continha o servidor *proxy*) ocorreu por meio de um roteador Wi-fi comum (marca Huawei, modelo HG8245H), em um canal sem fio (*wireless*).

3.4 FERRAMENTAS UTILIZADAS

Nesta seção serão apresentas as principais ferramentas utilizadas durante a análise dos aplicativos móveis do governo brasileiro.

Android Debug Bridge (adb)

É uma ferramenta de linha de comando que permite a comunicação com um dispositivo móvel (Android Developers, 2020). Toda a comunicação entre o dispositivo *host* e o dispositivo móvel foi realizada por meio de uma conexão pelas portas *USB* dos dispositivos, utilizando a ferramenta `adb`. Essa ferramenta foi utilizada para executar uma série de ações no dispositivo móvel, como instalar e remover aplicativos, realizar o backup de dados de um aplicativo, consultar o *log* do sistema móvel, entre outras atividades.

Apktool

É uma ferramenta de engenharia reversa de aplicativos binários Android (Apktool, 2020). Neste estudo, foi utilizado o Apktool versão 2.0.5 para decodificar os artefatos do aplicativo durante a análise estática.

Quando os aplicativos Android são criados todos os recursos necessários para sua instalação e execução são empacotados em um único arquivo no formato *Android Application Pack*, abreviado com o nome "APK". Pode-se visualizar o conteúdo de um arquivo "APK" utilizando ferramentas comuns de extração de arquivos "ZIP", tal como "7Zip". Ao extrair um arquivo "APK" é possível encontrar arquivos como `AndroidManifest.xml`, `classes.dex`, `resources.arsc`, entre outros. No entanto, tais arquivos estão codificados, não sendo possível a visualização do seu conteúdo. A fim de decodificar esses artefatos para a inspeção, foi o utilizada a ferramenta Apktool.

[4] `https://docs.mitmproxy.org`

Após a decodificação de um aplicativo Android, através do Apktool, geralmente, se encontram os seguintes arquivos e pastas no diretório de saída:

- `AndroidManifest.xml`: o arquivo de manifesto decodificado. O arquivo XML de manifesto contém informações essenciais sobre o aplicativo;
- `apktool.yml`: arquivo contendo informações sobre a saída da ferramenta Apktool;
- `original`: pasta que contém informações sobre os arquivos originais;
- `res`: diretório que contém os recursos do aplicativo (ex. imagens);
- `smali`: diretório contendo a decodificação de arquivos *Java* compilados para a forma de arquivos *smali*. Maiores informações sobre arquivos *smali* podem ser obtidas em sua documentação[5].

Android Backup Extractor

Quando é realizado o backup de um aplicativo através da ferramenta ADB a saída é um arquivo com extensão "*.ab*". Um arquivo de backup (*.ab*) é um arquivo comprimido com algumas características próprias. Para extrair o conteúdo do arquivo de backup foi utilizada a ferramenta Android Backup Extractor[6] (versão 20210709062403-4c55371). Essa ferramenta requer o Java JDK instalado. Nesse experimento foi utilizado o Java JDK 1.8.

Frida

Frida é considerado um kit de ferramentas de instrumentação dinâmica para desenvolvedores, pesquisadores de segurança e engenharia reversa (Ravnas, 2022). Essa ferramenta possui várias funcionalidades, como: enumerar funções, realizar o *hooking* de funções, enumerar bibliotecas carregadas, ler e gravar dados na memória do dispositivo, entre outros.

A ferramenta pode ser utilizada tanto em dispositivos *rooted*, fazendo o uso do recurso `frida-server`, como também em dispositivos não *rooted*, reempacotando o aplicativo com o recurso `frida-gadget`. Neste estudo, a ferramenta Frida (versão 15.1.17) foi utilizada para contornar a proteção *SSL Pinning* de alguns aplicativos, para tal, foi utilizado o modo de instrumentação para dispositivos *rooted*. Todos os detalhes sobre a ferramenta podem ser obtidos em sua documentação oficial[7].

---

[5] `https://github.com/JesusFreke/smali`
[6] `https://github.com/nelenkov/android-backup-extractor`
[7] `https://frida.re/docs/`

Exodus core

Exodus core[8] é uma ferramenta desenvolvida em linguagem *python* pela empresa Exodus Privacy (2021), uma organização sem fins lucrativos focada em compreender o problema do rastreamento de aplicativos. Conforme visto na Seção 3.2, um rastreador (*tracker*) é um software cuja função é coletar informações sobre quem usa o aplicativo, como usa ou sobre o smartphone que está em uso.

Neste estudo, foi utilizada a ferramenta Exodus Core (versão 1.3.5) para verificar a existência de rastreadores (*trackers*) nos aplicativos móveis do governo brasileiro. Vale notar que essa ferramenta também é utilizada internamente pela ferramenta de análise automatizada MobSF, para análise de rastreadores.

Mitmproxy

Mitmproxy[9] é um conjunto de ferramentas que fornece um servidor *proxy* de interceptação compatível com HTTP e HTTPS. Conforme visto na Seção 3.2, foi instanciado no dispositivo *host* um servidor *proxy* com o propósito de inspecionar o tráfego de dados entre o aplicativo móvel e servidores remotos.

Neste estudo, foi utilizado a ferramenta de linha de comando `mitmdump`, do Mitmproxy (versão 7.0.4). Optou-se por utilizar essa ferramenta em decorrência da praticidade oferecida pela linha de comando, possibilidade de personalização dos detalhes de captura e pelo seu reconhecimento pela comunidade.

3.5 MÉTODO DE ANÁLISE

Nesta seção é apresentado o método utilizado nesta pesquisa para analisar os aplicativos móveis do governo brasileiro.

As atividades que compõem o método de análise dos aplicativos selecionados nesta pesquisa são apresentadas na figura 3.2. Nota-se que abaixo de algumas atividades são apresentados os critérios de segurança e privacidade analisados pela atividade, conforme critérios estabelecidos na tabela 3.2. O método envolveu uma combinação entre atividades de análise estática (manual e automatizada) e atividades de análise dinâmica. A análise dinâmica foi utilizada para verificar o comportamento dos aplicativos e para inspecionar o tráfego de dados entre o aplicativo móvel e servidores remotos.

[8] `https://github.com/Exodus-Privacy/exodus-core`
[9] `https://mitmproxy.org/`

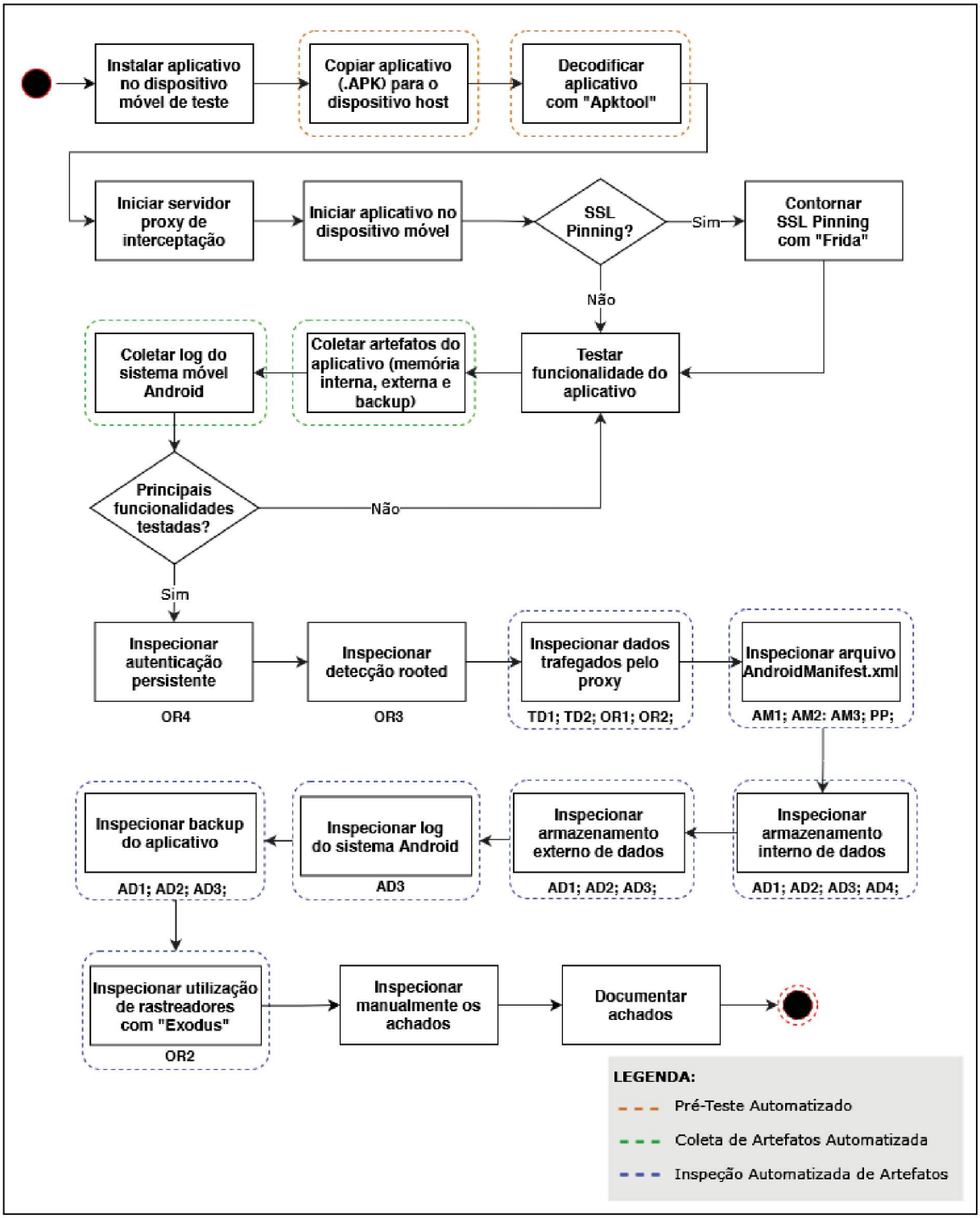


Figura 3.2: Método de análise dos aplicativos utilizado neste estudo.

Foram desenvolvidos pelo próprio pesquisador *scripts* de automatização de algumas atividades recorrentes. Os *scripts* foram criados com o propósito de otimizar o tempo, a qualidade e para padronização das atividades de análise. Cada atividade automatizada gera um artefato de *log* de sua execução, mantendo um histórico da análise de cada aplicativo. Na figura 3.2, é possível observar algumas atividades com linhas coloridas tracejadas ao redor, indicando que se tratam de atividades automatizadas pelos *scripts* do pesquisador, sendo as demais atividades realizadas de forma manual. As linhas tracejadas na cor amarela referem-se a atividades automatizadas e realizadas pré-teste, isto é, antes da execução do aplicativo no dispositivo móvel. As linhas tracejadas na cor verde referem-se a atividades de coleta de artefatos do aplicativo e do sistema móvel, sendo coletados dados de armazenamento interno, externo (cartão de memória removível), de backup do aplicativo (quando permitido) e de *log* do sistema móvel Android. Já as linhas tracejadas na cor azul referem-se a atividades de inspeção automatizada dos artefatos coletados, a fim de verificar o atendimento aos critérios de segurança e privacidade estabelecidos.

3.5.1 Busca por dados sensíveis

É relevante no presente estudo o método utilizado nas atividades de inspeção para localizar dados sensíveis do usuário e do aplicativo nos artefatos coletados, que possam vir a revelar possíveis vulnerabilidades de segurança e privacidade.

Este estudo optou por utilizar a técnica de busca por palavras-chave, que é uma das principais ferramentas utilizadas para identificar evidências relevantes em um conjunto de dados. Essa técnica pode ser bastante poderosa, especialmente quando as consultas de pesquisa são bem elaboradas. A busca eficaz por palavras-chave requer certa experiência e pode ser bastante ineficaz se não for utilizada de forma adequada. Essa técnica apresenta os seguintes dilemas: *Poucos resultados* - caso não seja possível prever as palavras-chave exatas que levem a evidências relevantes, podendo perder-se evidências importantes. Um simples erro de digitação pode afetar substancialmente os resultados; *Muitos resultados* - grandes listas de palavras-chave, na tentativa de capturar todas as evidências, pode retornar grande volume de dados irrelevantes. A revisão de falsos positivos consome muito tempo e pode ser bastante entediante.

Para auxiliar na busca por evidências relevantes nos artefatos coletados, foi criada uma lista de palavras-chave com dados sensíveis do usuário e do dispositivo móvel. Com relação ao usuário, foram incluídos dados como: *nome, sobrenome, data de nascimento, endereço, número de telefone fixo e móvel, números de documentos (RG, CPF, carteira de motorista, etc.), dados de veículos do usuário (marca, modelo, placa, número RENAVAM, etc.) e dados profissionais (nome, razão social, CNPJ de empresas contratantes, etc.)*. Com relação ao equipamento, foram incluídos dados como: *identificador único, número serial, número IMEI e dados de geolocalização (latitude, longitude)*. Alguns dados foram duplicados na listagem com suas variações, ou seja, com/sem pontuação e caracteres especiais.

Um *script* em linguagem *python* foi desenvolvido para automatizar a busca por palavras-chave em cada um dos artefatos coletados. Esse *script* percorre os artefatos, como dados de *log*, dados de *cache*, dados de tráfego de rede, dados de backup, bancos de dados e entre outros tipos de arquivos, em busca de palavras-chave presentes na listagem definida, gerando um relatório dos termos localizados. Esse *script* também lista arquivos em formatos conhecidos (como bancos de dados, imagens, arquivos PDF, entre outros) que podem conter evidências relevantes e merecem uma inspeção manual. O *script* de automatização otimiza bastante a busca por evidências relevantes nos artefatos coletados, porém, foi importante a utilização de inspeção manual a fim de validar os resultados e ajustar possíveis inconsistências.

3.5.2 Problemas na busca por palavras-chave

A busca por palavras-chave é uma ferramenta poderosa, no entanto, este estudo observou alguns problemas comuns no uso desta técnica: a codificação de dados e arquivos, a quantidade de falsos positivos e a ausência de termos importantes na lista de palavras-chave.

Nem todos os dados podem ser facilmente pesquisados. Muitas vezes, eles devem ser primeiro decodificados e apresentados em uma forma pesquisável. Por exemplo, desenvolvedores de aplicativos podem utilizar arquivos ou dados em diferentes codificações, como base16 (hexadecimal), base32, base64, entre outros. Diferentes tipos de codificação podem ser utilizados para propósitos distintos, seja em uma tentativa simples de ofuscar o armazenamento de dados sensíveis ou para compressão de dados e arquivos. Outro problema ocorre com arquivos de imagens contendo conteúdo textual, nesse caso, seria necessário realizar previamente o procedimento de reconhecimento óptico de caracteres (*Optical Character Recognition - OCR*), a fim de tornar o conteúdo do arquivo pesquisável. O tratamento de diferentes tipos de codificação não foi realizado neste estudo e seria um relevante aperfeiçoamento para uma pesquisa futura. Já o problema de imagens com conteúdo textual foi resolvido com a análise manual do conteúdo das imagens.

Os resultados falsos positivos são característicos em buscas palavras-chave e estão diretamente relacionados às palavras escolhidas. Como apresentado anteriormente, a razão óbvia pela qual falsos positivos são um problema é porque a revisão desses resultados podem consumir muito tempo e ser bastante entediante. Notou-se que alguns dados numéricos, por exemplo, números de documentos e data de nascimento, podem gerar muitos falsos positivos. O uso de palavras genéricas, como "senha" e "password", em uma tentativa de localizar o armazenamento da senha do usuário, também podem produzir muitos resultados falsos positivos. Apesar de a senha do pesquisador, utilizada para autenticação em alguns aplicativos, fazer parte da lista de palavras-chave pesquisadas, foram também pesquisadas palavras genérias relativas a senha, com o propósito de cobrir o caso no qual a senha do usuário possa ter sido armazenada com algum tipo de ofuscação. No entanto, nesta pesquisa, palavras-chave genéricas foram utilizadas de forma equilibrada.

Evidentemente, a tarefa de estabelecer um conjunto de palavras-chave perfeito é bastante improvável. É esperada a ausência de alguns termos que possam revelar o armazenamento de dados sensíveis do usuário ou do equipamento. Deste modo, esta pesquisa apoia-se na inspeção manual e na abstração do *Princípio de localidade de referência* (Denning, 1968), para resolver esse problema. Esse princípio foi proposto no contexto de Arquitetura de Computadores e acredita que ao longo da execução de um programa, as referências feitas à memória pelo processador tendem a formar grupos, nos quais elas estão próximas umas das outras. Deste modo, este estudo considera que os dados sensíveis tendem a ser armazenados próximos uns dos outros, de forma que uma palavra-chave esquecida esteja próxima a outras que foram contempladas, sendo evidenciada durante a inspeção manual.

Este Capítulo apresentou os parâmetros para seleção dos aplicativos móveis do governo brasileiro, os critérios de segurança e privacidade avaliados, o método e as ferramentas utilizadas nesta pesquisa. No Capítulo 4, são apresentados e discutidos os resultados da análise dos quatorze critérios de segurança e privacidade para os trinta aplicativos móveis selecionados.

4 RESULTADOS E DISCUSSÃO

Os resultados da análise dos trinta aplicativos do governo brasileiro são apresentados e discutidos neste Capítulo. As tabelas 4.4 e 4.5, ao final deste Capítulo, consolidam os quatorze critérios de segurança e privacidade avaliados para os aplicativos móveis do governo brasileiro.

Os aplicativos são apresentados de forma anonimizada e alguns achados importantes foram omitidos a fim de preservar a segurança dos aplicativos, pois a divulgação permitira revelar a sua identidade. O relatório detalhado de vulnerabilidades encontra-se no Apêndice A, o qual será mantido em sigilo por um prazo definido, conforme esclarecido na Seção 1.4.

Arquivo de manifesto

Observou-se que 70% dos aplicativos permitiram o backup de dados do aplicativo (AM1/OWASP-M2), podendo expor dados sensíveis armazenados sem a devida proteção. Por exemplo, nos arquivos de backup de determinados aplicativos foi possível obter diversos dados sensíveis do usuário, como: *nome completo, sexo, data de nascimento, raça, endereço, telefone, e-mail, número de CPF, dados de contrato de trabalho e dados de saúde*.

Identificou-se ainda que 86% dos aplicativos estavam configurados para permitir o tráfego de dados de forma insegura (não criptografados), inclusive de bibliotecas de terceiros (AM3/OWASP-M3). Desta forma, em uma rede sem a devida proteção, um adversário poderia inspecionar os dados trafegados pelo aplicativo, comprometendo a privacidade do usuário. No entanto, notou-se que todos os aplicativos atenderam positivamente o critério de desativar a configuração de depuração do aplicativo (AM2/OWASP-M7), isso se deve à exigência da própria loja para a publicação de aplicativos Android.

Armazenamento de dados

Nenhum aplicativo atendeu todos os quatro critérios de armazenamento seguro de dados. Observou-se que 86% dos aplicativos armazenaram dados sensíveis do usuário e do próprio aplicativo de forma insegura (AD1/OWASP-M2). Alguns aplicativos armazenaram esses dados inclusive no cartão de memória (dispositivo de armazenamento externo), podendo ser facilmente acessível por um adversário com acesso físico ao dispositivo. Os dados armazenados de forma insegura (não criptografados) estavam em diferentes formatos de arquivos, tais como: arquivos de banco de dados SQLite, arquivos XML, arquivos de imagem JPG, arquivos PDF, entre outros; conforme as imagens 4.1 a 4.3.

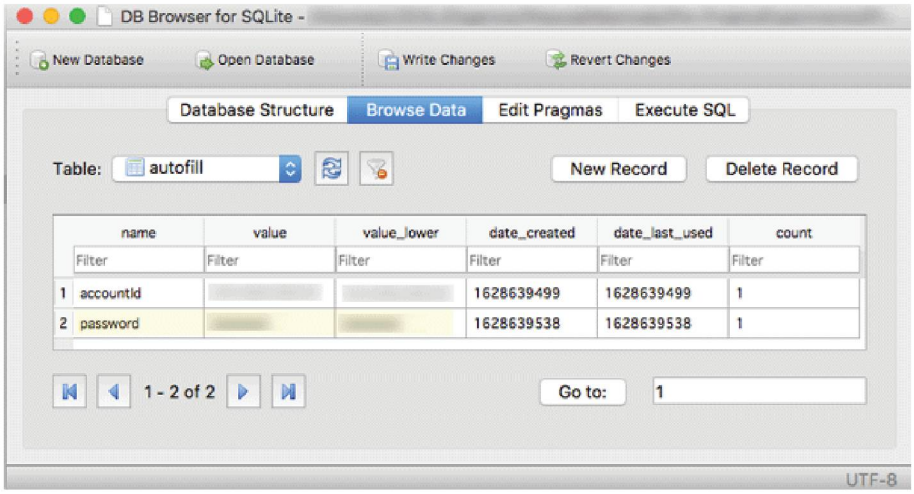


Figura 4.1: Banco de dados SQLite contendo número de CPF e senha do usuário em texto claro (não criptografados).

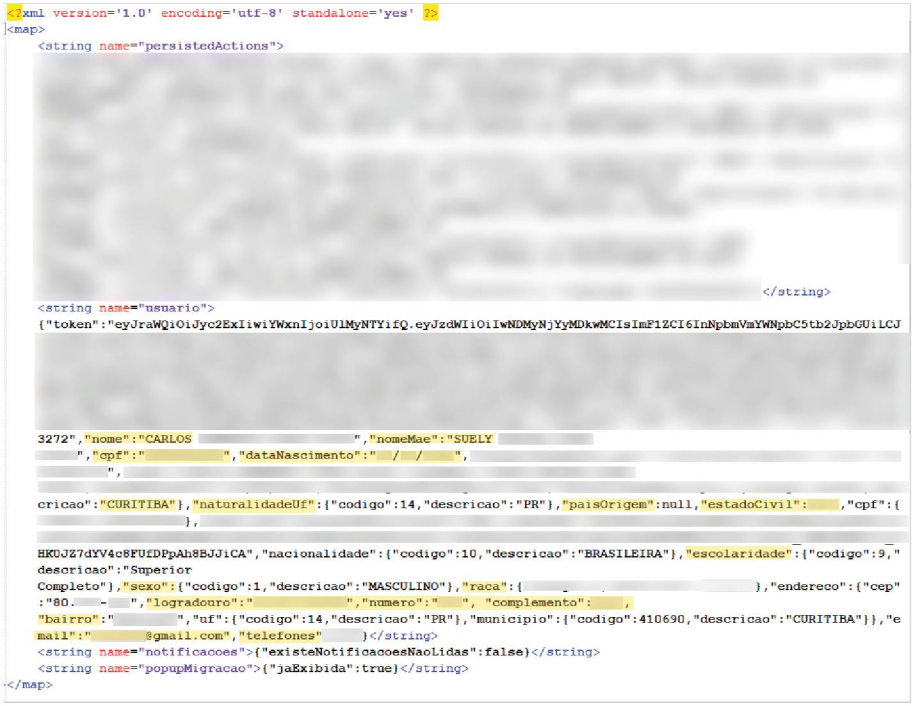


Figura 4.2: Arquivo XML contendo diversos dados do usuário em texto claro (não criptografados).

Figura 4.3: Arquivo PDF (encontrado no cartão de memória) contendo diversos dados do usuário em texto claro.

Identificou-se ainda que 53% dos aplicativos armazenaram dados sensíveis em arquivos *cache* (AD2/OWASP-M2). Mediante análise do tráfego de rede entre os aplicativos e os servidores remotos, verificou-se que, em alguns casos, os desenvolvedores não instruíram corretamente o aplicativo a não manter *cache* de dados sensíveis por meio da diretiva `Cache-Control`, conforme figura 4.4.

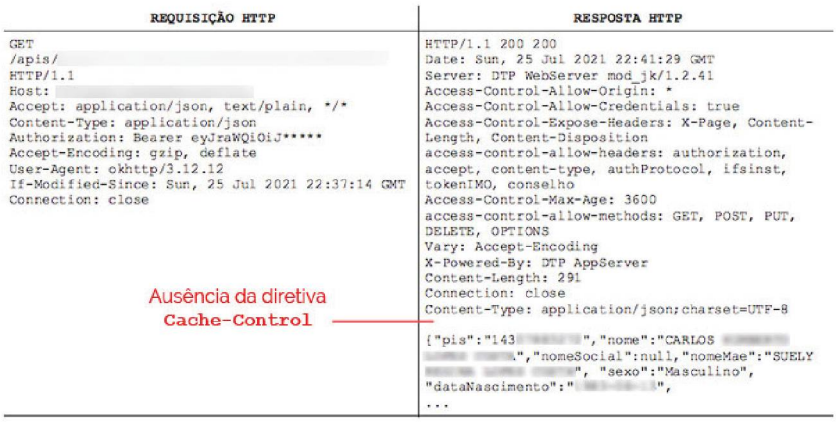


Figura 4.4: Requisição HTTPS contendo dados do usuário e com ausência de controle de cache.

Notou-se que 56% dos aplicativos armazenaram dados sensíveis em arquivos de *log* ou no *log* do sistema móvel (AD3/OWASP-M2), conforme figuras 4.5 e 4.6 . Observou-se ainda que cinco aplicativos (A3, A9, A17, A23 e A24), que utilizaram a biblioteca `ReactNativeJS`, registraram dados sensíveis no *log* do sistema móvel Android, possivelmente, devido aos desenvolvedores não terem configurado adequadamente a biblioteca. Cabe ressaltar que até mesmo a senha de autenticação do usuário foi registrada no *log* do sistema móvel sem a devida proteção, conforme figura 4.7. O registro em *log* de dados sensíveis é um enorme risco, pois pode expor dados a adversários ou aplicativos maliciosos, violando a privacidade do usuário (Mueller et al., 2020).

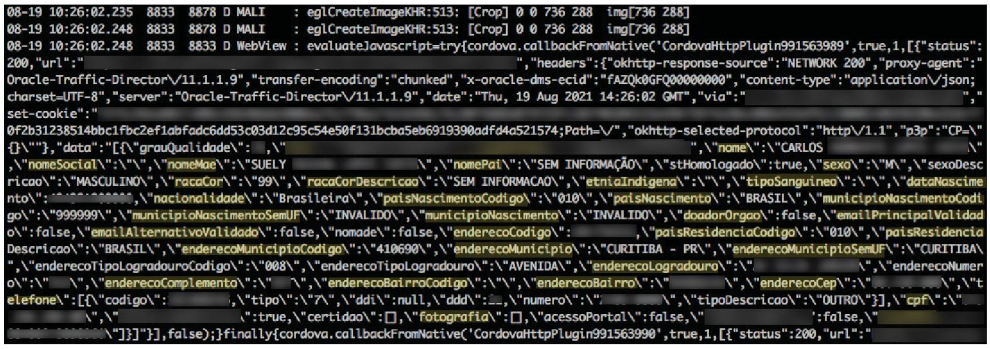


Figura 4.5: Log do sistema móvel Android com dados sensíveis do usuário, registrados por um dos aplicativos.

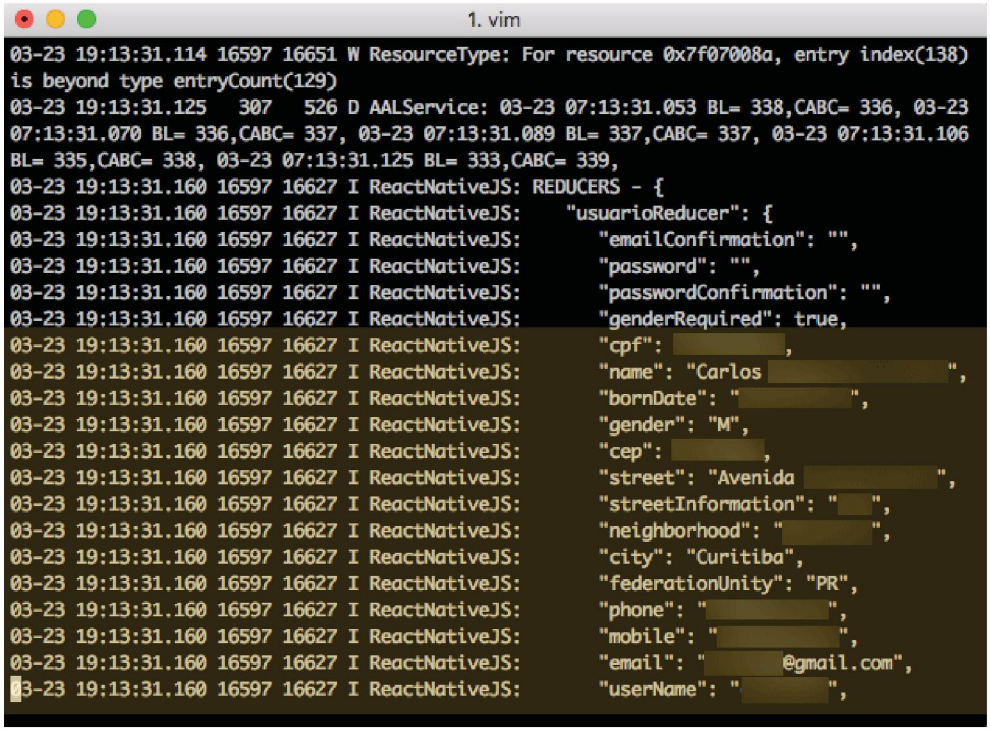


Figura 4.6: Log do sistema móvel Android com dados sensíveis do usuário, registrados por um dos aplicativos.

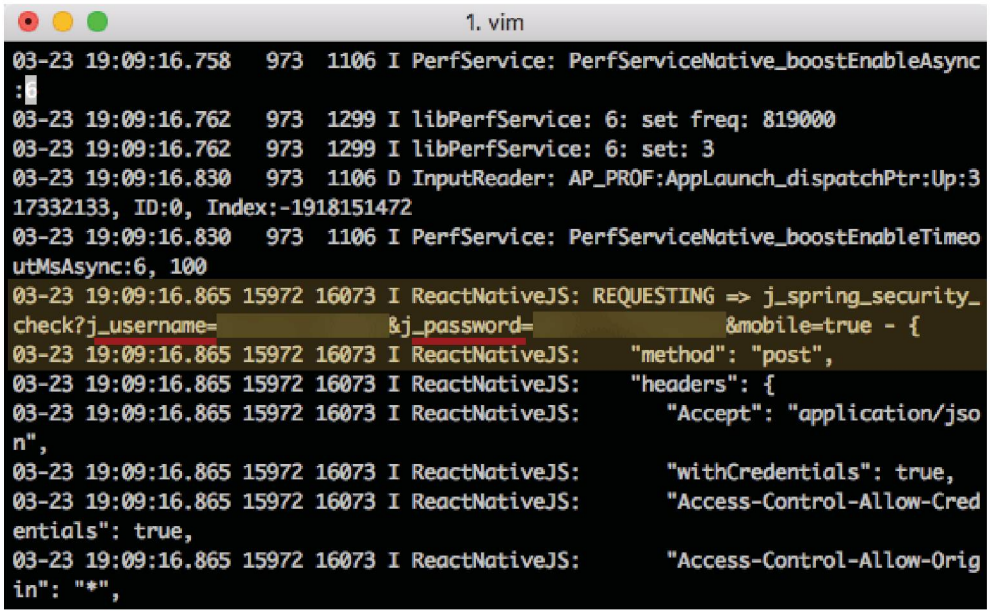


Figura 4.7: Log do sistema móvel Android com login e senha do usuário, registrados por um dos aplicativos.

Observou-se que nenhum aplicativo impediu o armazenamento de dados sensíveis em captura automática de tela do Android (AD4/OWASP-M2). Para fornecer uma experiência esteticamente agradável na transição entre aplicativos, o Android utiliza um recurso de captura automática de tela. Este recurso captura e armazena a tela do dispositivo, sempre que um aplicativo é colocado em segundo plano. Deste modo, a privacidade do usuário pode ser comprometida, se a captura de tela ocorrer enquanto o aplicativo exibe dados sensíveis do usuário.

Observou-se ainda que sete aplicativos (A3, A9, A11, A17, A24, A25 e A27) não atenderam nenhum dos quatro critérios de armazenamento de dados. Vale notar que um desses aplicativos manipula dados bastante sensíveis do usuário.

Este trabalho identificou diversos dados sensíveis que poderiam ser expostos pelos aplicativos do governo brasileiro, em decorrência de serem armazenados sem a devida proteção, conforme tabela 4.1. Cabe ressaltar que alguns dados bastante sensíveis que poderiam ser expostos não constam nesta tabela, a fim de preservar os aplicativos, pois o mesmo poderia ser facilmente identificado.

Tabela 4.1: Alguns dados sensíveis armazenados sem a devida proteção.

Dados
Nome completo
Nome social
Nome da mãe
Sexo
Data de nascimento
Número de CPF
Número PIS
Endereço de e-mail
Número de telefone
Raça/Cor
Tipo sanguíneo
Endereço residencial
Fotografia
Senha de autenticação ao serviço Gov.br
Dados do dispositivo e do aplicativo (número de série, marca/modelo do dispositivo, número IMEI, token de autenticação, entre outros)

Transmissão de dados

Notou-se que 79% dos aplicativos trafegaram corretamente dados em um canal de comunicação seguro/criptografado (TD1/OWASP-M3) e 72% adotaram corretamente medidas de proteção da comunicação com a técnica "SSL Pinning" (TD2/OWASP-M3).

No entanto, utilizando um dispositivo *rooted*, foi possível contornar a proteção "SSL Pinning" e inspecionar os dados trafegados em praticamente todos os aplicativos, com exceção de um único aplicativo, no qual não foi possível aplicar a técnica de contorno utilizando a ferramenta Frida, descrita na Seção 3.4. O *rooting* de dispositivos é um comportamento inseguro que deve ser previsto pelos desenvolvedores de aplicativos, conforme abordado na Seção 2.5.

Permissões perigosas

Observou-se que 90% dos aplicativos não adotaram boas práticas na solicitação de "permissões perigosas" (PP/OWASP-M1), as quais dão acesso a dados restritos dos usuários. Tais permissões foram solicitadas grande parte das vezes sem que o usuário fosse informado sobre a necessidade da permissão. O aplicativo "A2" foi o que mais solicitou permissões perigosas, com um total de sete, conforme figura 4.8. Apenas três aplicativos não solicitaram permissões perigosas sem necessidade (As21, A7 e A27). As "permissões perigosas" mais solicitadas foram de leitura e gravação no dispositivo de armazenamento externo (`READ_EXTERNAL_STORAGE / WRITE_EXTERNAL_STORAGE`), ou seja, no cartão de memória externo, solicitadas por 25 aplicativos, seguidas pela permissão de acesso à câmera do dispositivo (`CAMERA`), solicitada por 13 aplicativos, conforme figura 4.9.

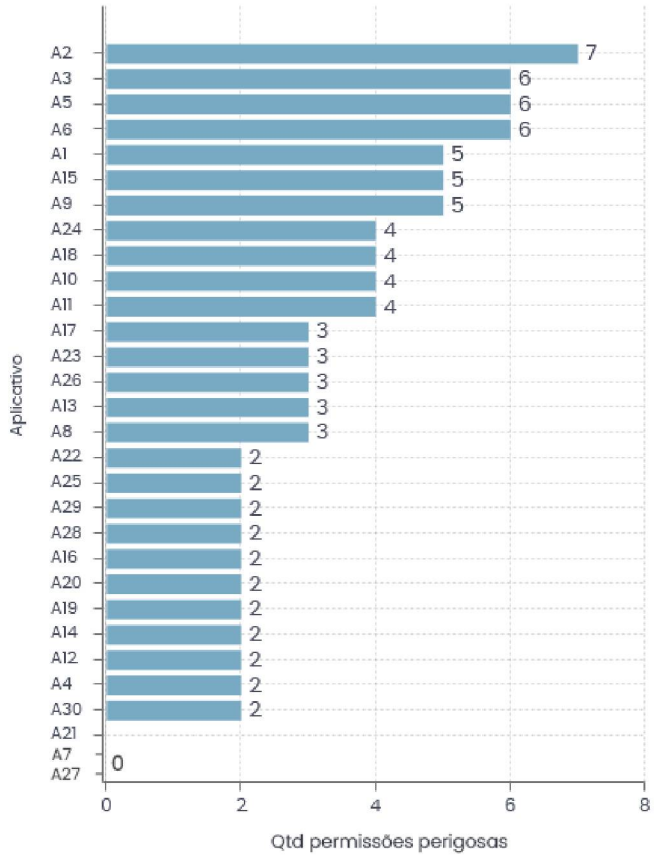


Figura 4.8: Qtd. de Permissões Perigosas por Aplicativo.

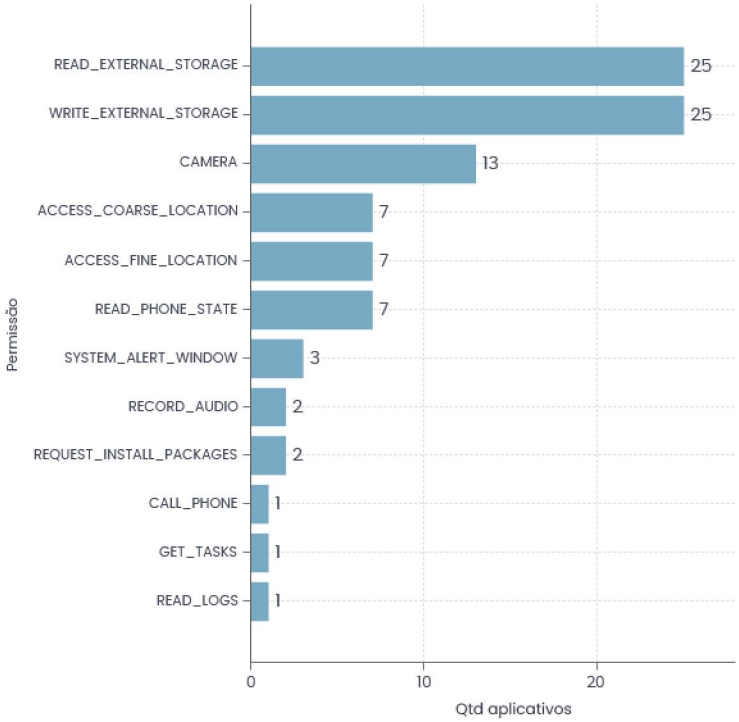


Figura 4.9: Qtd. Aplicativos que solicitaram determinada "Permissão Perigosa".

Despertou a atenção o fato de dois aplicativos "A1" e "A2" solicitarem permissão para gravação de áudio (`RECORD_AUDIO`) e outros sete aplicativos solicitarem permissão para ter acesso ao estado e identificações do aparelho (`READ_PHONE_STATE`), tal como se há ligações ativas, qual número está ligando para o usuário e qual o número de telefone do equipamento.

Na figura 4.10, podemos observar que o aplicativo "A24" utilizou a permissão "`READ_PHONE_STATE`" para coletar dados do dispositivo (número IMEI, número de telefone, modelo do dispositivo, entre outros) e ainda registrou de forma insegura esses dados no log do Android. Na tabela 4.2 podemos verificar um resumo das "permissões perigosas" solicitadas por cada aplicativo.

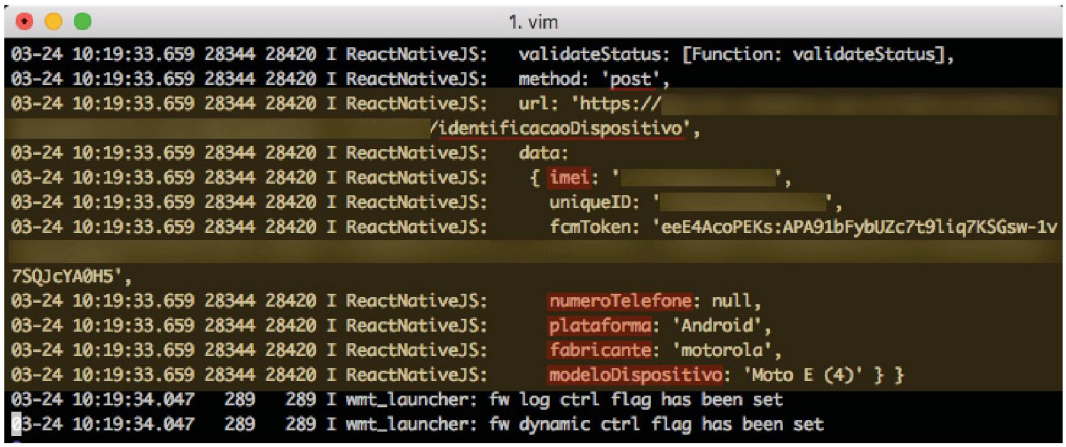


Figura 4.10: Log do sistema móvel Android contendo dados coletados do dispositivo pelo aplicativo "A24".

Tabela 4.2: Resumo das permissões perigosas solicitadas pelos aplicativos.

Aplicativo	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12
A1				✓		✓			✓	✓		✓
A2	✓			✓		✓		✓	✓		✓	✓
A3	✓	✓		✓		✓		✓				✓
A4						✓						✓
A5	✓	✓	✓	✓		✓						✓
A6	✓	✓		✓		✓		✓				✓
A7												
A8		✓		✓			✓					
A9				✓		✓		✓			✓	✓
A10	✓	✓				✓						✓
A11						✓		✓		✓		✓
A12						✓						✓
A13				✓		✓						✓
A14						✓						✓
A15	✓	✓		✓		✓						✓
A16						✓						✓
A17				✓		✓						✓
A18	✓	✓			✓			✓				
A19						✓						✓
A20						✓						✓
A21				✓								
A22						✓						✓
A23				✓		✓						✓
A24						✓		✓			✓	✓
A25						✓						✓
A26				✓		✓						✓
A27												
A28						✓						✓
A29						✓						✓
A30						✓						✓

P1. ACCESS_COARSE_LOCATION
P2. ACCESS_FINE_LOCATION
P3. CALL_PHONE
P4. CAMERA
P5. GET_TASKS
P6. READ_EXTERNAL_STORAGE
P7. READ_LOGS
P8. READ_PHONE_STATE
P9. RECORD_AUDIO
P10. REQUEST_INSTALL_PACKAGE
P11. SYSTEM_ALERT_WINDOW
P12. WRITE_EXTERNAL_STORAGE

Outros riscos

Observou-se que 63% dos aplicativos incorporaram serviços de terceiros, muitas vezes sem o conhecimento do usuário, podendo comprometer a sua privacidade (OR1/OWASP-M2). Foram identificadas configurações para o serviço de nuvem *Firebase*[1] em 15 dos aplicativos avaliados. Esse serviço é comumente utilizado para armazenar e sincronizar dados em tempo real. Identificou-se ainda o compartilhamento de dados com o serviço *OneSignal*[2] em 2 aplicativos. A figura 4.11 apresenta um aplicativo compartilhando dados do dispositivo do usuário com o serviço *OneSignal*, como o modelo do equipamento, a versão do sistema operacional, o indicativo se o dispositivo está *rooted*, entre outros, violando a privacidade do usuário, uma vez que não é transparente para o usuário quais dados o aplicativo irá coletar e com quais serviços irá compartilhar tais dados.

```
2022-03-21 15:59:08.707: 192.168.100.36:32868: POST https://api.onesignal.com/players
    SDK-Version: onesignal/android/031501
    Accept: application/vnd.onesignal.v1+json
    Content-Type: application/json; charset=UTF-8
    Content-Length: 344
    User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.1.1; Moto E (4) Build/NMA26.42-169)
    Host: api.onesignal.com
    Connection: Keep-Alive
    Accept-Encoding: gzip
    {<CR>
        "ad_id": "                                    ",<CR>
        "android_package": "br.com.                   ",<CR>
        "app_id": '                                    ",<CR>
        "device_model": "Moto E (4)",<CR>
        "device_os": "7.1.1",<CR>
        "device_type": 1,<CR>
        "game_version": 79,<CR>
        "language": "en",<CR>
        "net_type": 0,<CR>
        "notification_types": -9,<CR>
        "rooted": true,<CR>
        "sdk": "031501",<CR>
        "sdk_type": "cordova",<CR>
        "timezone": -14400<CR>
    }
 << 200 OK 86b
```

Figura 4.11: Aplicativo compartilhando dados do dispositivo do usuário com o serviço *OneSignal*.

Rastreadores (*trackers*) foram observados em 80% dos aplicativos (OR2/OWASP-M2), utilizados sem o conhecimento e o consentimento do usuário, podem comprometer a sua privacidade. Os rastreadores (*trackers*), conforme vimos na Seção 3.2, têm a função de coletar informações sobre quem usa um aplicativo e como usa e sobre o dispositivo que está em uso (conforme vimos na figura 4.11), podendo apresentar diferentes níveis de invasão de privacidade, conforme o tipo de rastreador.

A maior parte dos rastreadores identificados se enquadram na categoria "Analytics", responsáveis por coletar dados sobre o uso do aplicativo, para permitir ao desenvolvedor um melhor conhecimento de seu público. A segundo categoria mais utilizada foi os rastreadores "Crash reporters", que são especializados em relatar falhas em aplicativos.

[1] https://firebase.google.com/
[2] https://onesignal.com

Os aplicativos “A12” e “A15” foram os que mais utilizaram rastreadores, conforme figura 4.12. Apenas em 6 aplicativos não foram identificados rastreadores. O rastreador mais utilizado foi o “Google Firebase Analytics”, encontrado em 22 aplicativos, conforme figura 4.13. A tabela 4.3 apresenta um resumo dos rastreadores utilizados por cada aplicativo.

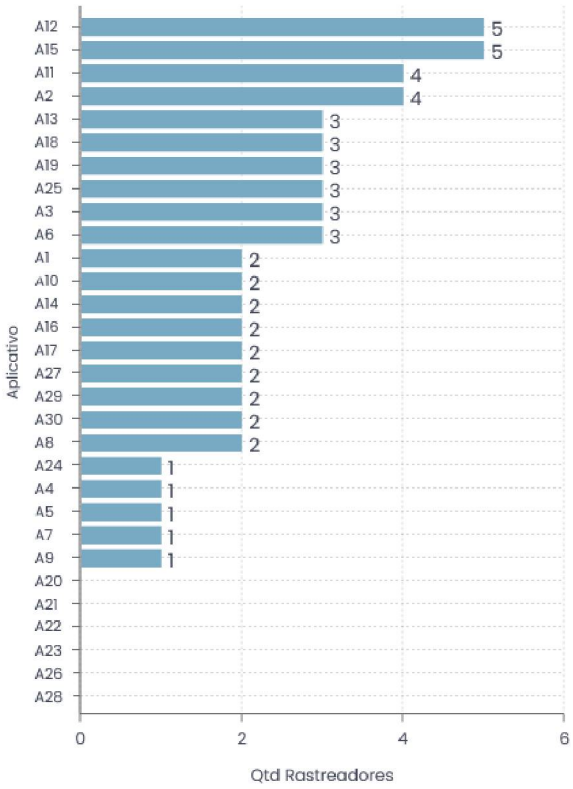


Figura 4.12: Qtd. de Rastreadores por Aplicativo.

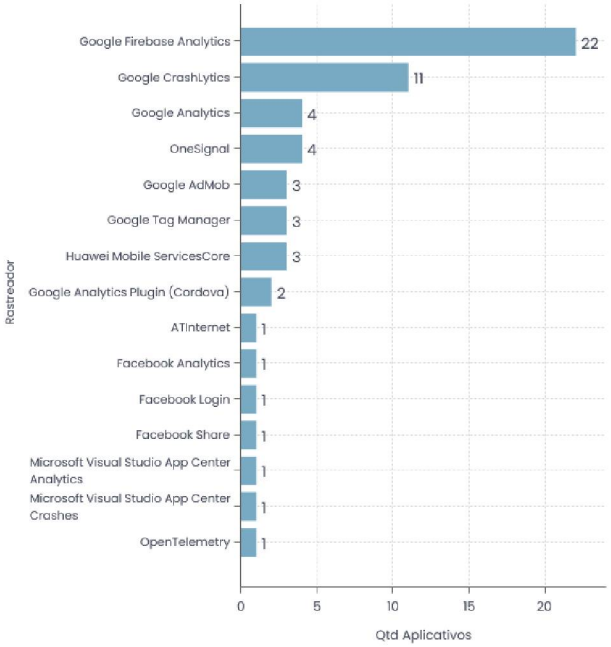


Figura 4.13: Qtd. de Aplicativos que utilizaram determinado Rastreador.

Tabela 4.3: Resumo dos rastreadores existentes nos aplicativos.

Aplicativo	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15
A1								✓	✓						
A2					✓			✓	✓						✓
A3					✓			✓	✓						
A4									✓						
A5									✓						
A6						✓	✓			✓					
A7									✓						
A8								✓	✓						
A9									✓						
A10								✓	✓						
A11						✓		✓	✓	✓					
A12						✓	✓		✓		✓			✓	
A13									✓		✓			✓	
A14								✓	✓						
A15	✓	✓	✓	✓					✓						
A16								✓	✓						
A17									✓					✓	
A18					✓	✓				✓					
A19									✓			✓	✓		
A20															
A21															
A22															
A23															
A24									✓						
A25									✓		✓			✓	
A26															
A27								✓	✓						
A28															
A29								✓	✓						
A30								✓	✓						

R1. ATInternet
R2. Facebook Analytics
R3. Facebook Login
R4. Facebook Share
R5. Google AdMob
R6. Google Analytics
R7. Google Analytics Plugin(Cordova)
R8. Google CrashLytics
R9. Google Firebase Analytics
R10. Google Tag Manager
R11. Huawei Mobile Services Core
R12. Microsoft Visual Studio App Center Analytics
R13. Microsoft Visual Studio App Center Crashes
R14. OneSignal
R15. OpenTelemetry

Nenhum aplicativo adotou proteção contra dispositivos *rooted* (OR3/OWASP-M8). Conforme vimos na Seção 3.2, um dispositivo *rooted* compromete os mecanismos de segurança do dispositivo e pode expor os dados do usuário a uma violação de privacidade (Casati e Visconti, 2018). Os desenvolvedores devem avaliar os impactos na segurança de seus aplicativos, caso os usuários utilizem dispositivos *rooted*.

Observou-se que apenas 34% dos aplicativos, que possuem autenticação de acesso, adotaram autenticação não persistente (OR4/OWASP-M4), isto é, exigem que o usuário se autentique a cada acesso. O esquema de autenticação persistente pode tornar os dados do usuário vulneráveis, uma vez que qualquer pessoa com acesso ao dispositivo poderia acessar dados sensíveis do usuário, sem a necessidade de uma nova autenticação. Segundo o *OWASP Mobile Top Ten 2016*, a utilização de autenticação persistente, habilitada por padrão, é um esquema de design de autenticação de aplicativo móvel inseguro.

Durante a realização dos experimentos desta pesquisa, despertou também a atenção um importante aplicativo do Governo Federal brasileiro ter sido desenvolvido com o construtor de aplicativos de um serviço estrangeiro. Vale notar ainda que a contratação desse serviço foi realizada por meio de Inexigibilidade de Licitação, conforme figura 4.14. Observou-se ainda que muitos aplicativos disponibilizaram link para a sua "Política de Privacidade", que deveria trazer informações sobre a coleta e compartilhamento de dados do usuário, no entanto, muitos destes links estavam indisponíveis, direcionavam o usuário para um conteúdo não relacionado ou exibiam uma política de privacidade genérica, que não trazia informações relevantes ao usuário.

DIÁRIO OFICIAL DA UNIÃO

Publicado em: Seção: 3 | Página 13

Órgão:

EXTRATO DE INEXIGIBILIDADE DE LICITAÇÃO

Inexigibilidade de Licitação nº - Processo: Objeto: Contratação de Software como serviço para desenvolvimento e manutenção do aplicativo oficial do - Construtor de aplicativos para dispositivos móveis GoodBarber. Total de itens: 01. Fundamento Legal: artigo 25, Caput, da Lei nº 8.666, de 21/06/1993. Justificativa: Inviabilidade de competição. Reconhecimento em 15/02/2021. Ordenador de Despesas. Ratificação em 15/02/2021. Valor Global: US$ Contratada: empresa GoodBarber.

Figura 4.14: Contratação de serviço estrangeiro para desenvolvimento de aplicativo móvel do governo brasileiro.

Os resultados da pesquisa evidenciam a necessidade de aprimorar as medidas de segurança e de proteção da privacidade dos aplicativos móveis do governo brasileiro, caso contrário, dados sensíveis de milhões de usuários brasileiros correm o sério risco de serem expostos indevidamente. As tabelas 4.4 e 4.5 consolidam os quatorze critérios de segurança e privacidade avaliados para os aplicativos móveis do governo brasileiro.

Tabela 4.4: Resumo da análise dos aplicativos móveis do governo brasileiro (aplicativos A1 a A15).

Critério atendido pelo aplicativo	**Risco OWASP**	**A1**	**A2**	**A3**	**A4**	**A5**	**A6**	**A7**	**A8**	**A9**	**A10**	**A11**	**A12**	**A13**	**A14**	**A15**
AM1: O atributo `allowBackup` está configurado de forma apropriada, não permitindo o backup de dados sensíveis	M2	✓							✓		✓				✓	✓
AM2: O atributo `debuggable` está configurado de forma apropriada para um aplicativo em versão de produção.	M7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AM3: O atributo `usesCleartextTraffic` está configurado de forma apropriada, não permitindo que o aplicativo e bibliotecas de terceiros trafeguem dados de forma insegura	M3							✓	✓							✓
AD1: Armazena dados sensíveis localmente de forma segura	M2						NA	NA								✓
AD2: Não armazena dados sensíveis em arquivos de cache	M2	✓				✓	NA	NA	✓		NA			✓	✓	✓
AD3: Não registra dados sensíveis em arquivos de *log* ou no *log* do sistema operacional	M2	✓	✓		✓		NA				✓		✓	✓		✓
AD4: Adota proteção contra a captura de dados sensíveis em auto-screenshots	M2															
TD1: Trafega dados em um canal de rede seguro (criptografado)	M3	✓	✓	✓	✓	✓	✓	✓	✓	✓	NA	✓		✓	✓	
TD2: Adota medida de proteção da comunicação de rede por *SSL Pinning*	M3	✓					✓	✓	✓	✓	✓	✓	✓		✓	
PP: Não solicita permissões perigosas além do mínimo necessário	M1							✓								
OR1: Não compartilha dados com terceiros	M2						✓	✓					✓			
OR2: Não utiliza rastreadores (*trackers*) que podem comprometer a privacidade do usuário	M2															
OR3: Adota medidas para detectar e responder adequadamente a um dispositivo *rooted*	M8															
OR4: Exige a autenticação do usuário a cada novo acesso ao aplicativo (não adota autenticação persistente)	M4	✓			✓		NA		✓		-	✓	NA			-

(NA) Não foi possível avaliar / (-) Não se aplica

Tabela 4.5: Resumo da análise dos aplicativos móveis do governo brasileiro (aplicativos A16 a A30).

Critério atendido pelo aplicativo	Risco OWASP	A16	A17	A18	A19	A20	A21	A22	A23	A24	A25	A26	A27	A28	A29	A30
AM1: O atributo `allowBackup` está configurado de forma apropriada, não permitindo o backup de dados sensíveis	M2	✓	✓						✓							✓
AM2: O atributo `debuggable` está configurado de forma apropriada para um aplicativo em versão de produção.	M7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AM3: O atributo `usesCleartextTraffic` está configurado de forma apropriada, não permitindo que o aplicativo e bibliotecas de terceiros trafeguem dados de forma insegura	M3			✓			-									
AD1: Armazena dados sensíveis localmente de forma segura	M2			NA	✓	✓	✓					NA				
AD2: Não armazena dados sensíveis em arquivos de cache	M2	✓		NA	✓	✓	✓	✓	✓					✓		✓
AD3: Não registra dados sensíveis em arquivos de *log* ou no *log* do sistema operacional	M2	✓		NA	✓	✓	✓	✓							✓	
AD4: Adota proteção contra a captura de dados sensíveis em auto-screenshots	M2			NA												
TD1: Trafega dados em um canal de rede seguro (criptografado)	M3	✓	✓	NA	✓	✓	-	✓	✓	✓	✓		✓		✓	✓
TD2: Adota medida de proteção da comunicação de rede por *SSL Pinning*	M3	✓	✓	NA	✓	✓	-	✓	✓	✓	✓	✓	✓		✓	✓
PP: Não solicita permissões perigosas além do mínimo necessário	M1						✓						✓			
OR1: Não compartilha dados com terceiros	M2			NA		✓	✓	✓	✓		✓	✓	✓	✓		
OR2: Não utiliza rastreadores (*trackers*) que podem comprometer a privacidade do usuário	M2					✓	✓	✓	✓			✓		✓		
OR3: Adota medidas para detectar e responder adequadamente a um dispositivo *rooted*	M8			NA												
OR4: Exige a autenticação do usuário a cada novo acesso ao aplicativo (não adota autenticação persistente)	M4	-	NA	NA	✓	-	-	-	✓			NA		✓	✓	-

(NA) Não foi possível avaliar / (-) Não se aplica

Este Capítulo apresentou os resultados da análise dos critérios de segurança e privacidade, estabelecidos na Seção 3.2, para os aplicativos móveis do governo brasileiro. Lembramos que o relatório detalhado de vulnerabilidades encontra-se no Apêndice A, o qual será mantido em sigilo por um prazo definido, conforme esclarecido na Seção 1.4. No Capítulo 5 apresentamos as conclusões desta pesquisa, realizamos algumas recomendações à Administração Pública e aos usuários e propomos alguns trabalhos futuros.

5 CONCLUSÃO

Neste Capítulo são apresentadas as conclusões e respostas as perguntas de pesquisa. Na sequência são realizadas recomendações à Administração Pública e aos usuários dos aplicativos. Por fim, são apresentadas as contribuições da pesquisa e propostos alguns trabalhos futuros.

5.1 RESPOSTAS ÀS PERGUNTAS DE PESQUISA

Os dispositivos móveis e aplicativos estão cada vez mais presentes no dia a dia dos usuários e para muitos brasileiros são o principal meio de acesso à internet. Consequentemente, o governo brasileiro passou a disponibilizar informações e serviços através de aplicativos móveis. Documentos oficiais já podem ser utilizados de forma digital, no celular, com a mesma validade dos documentos físicos. Centenas de outros aplicativos são disponibilizados nas lojas oficias do governo brasileiro, sendo que muitos destes lidam com dados pessoais e confidenciais.

Reconhecendo a necessidade de preservar os dados pessoais e confidencias dos usuários, buscou-se neste trabalho avaliar se os aplicativos móveis do governo brasileiro adotam mecanismos de segurança para preservar tais dados e se coletam ou compartilham outras informações, sem o devido consentimento do usuário. Assim sendo, a Seção 1.2 propôs duas perguntas como objetivo da pesquisa, as quais são respondidas a seguir:

A **Os dados pessoais e confidenciais dos usuários de aplicativos móveis do governo brasileiro podem ser expostos?**

Sim. Apresentados no Capítulo 4, os resultados apontam que nenhum dos aplicativos selecionados do governo brasileiro atenderam todos os critérios de segurança e privacidade estabelecidos. Esses aplicativos expuseram dados sensíveis do usuário, como: números de documentos, número de telefone, tipo sanguíneo, endereço residencial, dados profissionais, dados de saúde, senha de autenticação, entre outros.

B **Esses aplicativos móveis coletam dados desnecessários ou compartilham informações dos usuários brasileiros sem o devido consentimento?**

Sim. Os resultados demonstram que todos os aplicativos comprometeram a privacidade do usuário, seja solicitando permissões para acessar dados desnecessários do usuário e/ou compartilhando dados sensíveis com serviços de terceiros, sem o claro consentimento do usuário. Foram solicitadas permissões para gravação de áudio e para acesso ao status de ligações no dispositivo. Observou-se ainda que alguns aplicativos incorporam serviços de terceiros, como o *Firebase*, e que muitos utilizaram ao menos um rastreador (*tracker*), que pode coletar informações sobre o aplicativo, o dispositivo e/ou o usuário.

Concluiu-se a necessidade de aprimorar os mecanismos de segurança dos aplicativos do governo brasileiro, pois, atualmente, representam um risco à privacidade de milhões de usuários brasileiros.

5.2 RECOMENDAÇÕES À ADMINISTRAÇÃO PÚBLICA FEDERAL

Esta seção planejava fornecer recomendações ao governo brasileiro quanto ao desenvolvimento seguro de aplicativos móveis, no entanto, durante a realização desta pesquisa, foi publicado pelo Governo do Brasil, em 30/11/2021, o "*Guia de Requisitos Mínimos de Segurança e Privacidade para Aplicativos Móveis*" (Governo do Brasil, 2021b). Este guia tem o propósito de fomentar orientações básicas aos desenvolvedores de aplicativos da Administração Pública Federal sobre o desenvolvimento seguro dos aplicativos móveis, além de abordar uma metodologia de desenvolvimento que considere os preceitos de privacidade desde a concepção do aplicativo. A publicação deste guia foi uma agradável surpresa, visto que este vai ao encontro das necessidades de enfrentamento de vulnerabilidades identificadas nesta pesquisa.

Outras iniciativas também demonstram que o governo brasileiro caminha no sentido correto, como a publicação da Portaria nº 39, de 09/07/2019, que estabelece que o registro de aplicativos móveis nas lojas de aplicativos será realizado por meio de conta única do Governo Federal, facilitando a busca por aplicativos oficiais pelo cidadão, e a aprovação da "*Estratégia Nacional de Segurança Cibernética - E-Ciber*", Decreto nº 10.222, de 5 de fevereiro de 2020. A "*Estratégia Nacional de Segurança Cibernética - E-Ciber*" é uma orientação manifesta do Governo Federal à sociedade brasileira sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética e com validade no quadriênio 2020-2023. O trabalho foi coordenado pelo Gabinete de Segurança Institucional da Presidência da República, e contou com a participação de mais de quarenta órgãos e entidades do Governo, além de instituições privadas e do setor acadêmico.

Ainda assim, este estudo revelou a primordial necessidade de amadurecimento da Administração Pública Federal quanto à preservação da segurança e privacidade dos usuários de aplicativos móveis do governo brasileiro. Isto é evidenciado pelos achados desta pesquisa. Por exemplo, o "*Guia de Requisitos Mínimos de Segurança e Privacidade para Aplicativos Móveis*" do Governo do Brasil estabelece a seguinte orientação: "*Não armazenar dados sensíveis e chaves privadas, a menos que sejam criptografados e, se possível, armazenados de maneira anonimizada em uma área à prova de violação, com suporte pelo fabricante da plataforma.*" (pág.19), entretanto, foi observado o armazenamento de dados sensíveis de forma insegura em 86% dos aplicativos avaliados. Outra orientação é: "*Desativar o plano de fundo ou usar uma tela desfocada quando o aplicativo fizer a transição para o plano de fundo em plataformas que mantêm uma captura de tela da tela visível no armazenamento local*" (pág.23), no entanto, nenhum dos aplicativos adotou proteção contra a exposição de dados sensíveis em captura automática de tela.

O guia recomenda ainda "*Considerar barrar acesso root a funcionalidades do app que manipulem dados sensíveis, uma vez que malwares podem escalar privilégios no dispositivo e dessa forma adentrar em qualquer funcionalidade ou caixa de areia de qualquer app.*" (pág.29), no entanto, nenhum dos aplicativos adotou proteção contra dispositivos inseguros (*rooted*). Outra recomendação é "*Limpar todos os dados sensíveis mantidos e tente também encerrar qualquer sessão do lado do servidor após a mudança de estado do aplicativo (por exemplo, encerramento, segundo plano). Considere uma solicitação do usuário para o encerramento do aplicativo como uma solicitação de logout.*" (pág.29), porém, observou-se que apenas 34% dos aplicativos, que possuem autenticação de acesso, exigem que o usuário se re-autentique a cada novo acesso ao aplicativo.

Diante das descobertas desta pesquisa, recomenda-se:

- Divulgação e capacitação contínua das equipes quanto às práticas de desenvolvimento seguro de aplicativos móveis;
- Capacitação contínua de equipes de auditoria de segurança e privacidade de aplicativos móveis;
- Realização de auditoria contínua e sistemática da segurança e privacidade dos aplicativos, de modo a garantir que estão sendo seguidos os requisitos estabelecidos;
- Manutenção contínua do "Guia de Requisitos Mínimos de Segurança e Privacidade para Aplicativos Móveis", considerando que segurança cibernética é um assunto bastante volátil;
- Elaboração de normativa que estabeleça a obrigatoriedade dos aplicativos móveis do governo brasileiro de atenderem aos requisitos de segurança e privacidade estabelecidos;
- Elaboração de campanhas públicas de conscientização da sociedade em segurança cibernética;

A capacitação quanto ao desenvolvimento seguro de aplicativos é muito importante, pois os desenvolvedores estão acostumados a tomar decisões sobre a arquitetura de seus aplicativos, com enfoque nas funcionalidades, contudo, as demandas de privacidade e proteção dos dados raramente são priorizadas *(European Union Agency For Network and Information Security, 2018)*. Considerando que os aplicativos móveis estão expostos a um conjunto distinto de ameaças, é indispensável também a definição de um processo de análise sistemática da segurança e privacidade dos aplicativos, pois é uma das maneiras mais eficazes de identificar pontos fracos conhecidos e desconhecidos e *bug* em funcionalidades (que podem levar a uma vulnerabilidade). Devido à constante evolução tecnológica, é fundamental que tais iniciativas façam parte de um processo de melhoria contínua.

Ademais, sugere-se a elaboração de uma Portaria que estabeleça a obrigatoriedade da aplicação de normas de segurança e privacidade para os aplicativos móveis de governo brasileiro. Vale notar que Portaria é um importante instrumento pelo qual o Ministro de Estado ou outra autoridade estabeleça instruções e procedimentos de caráter geral necessários à execução de leis, decretos e regulamentos (Governo do Brasil, 2017). Deste modo, passaria a se tornar obrigatório o cumprimento por parte dos aplicativos móveis do governo brasileiro dos requisitos estabelecidos no "*Guia de Requisitos Mínimos de Segurança e Privacidade para Aplicativos Móveis*" (Governo do Brasil, 2021b).

Destaca-se que as recomendações propostas e baseadas nos achados desta pesquisa estão em concordância com a "*Estratégia Nacional de Segurança Cibernética - E-Ciber*" e, em especial, com as seguintes ações estratégicas: "*2.3.4. Elevar o nível de proteção do Governo*", "*2.3.5. Elevar o nível de proteção das Infraestruturas Críticas Nacionais*", "*2.3.6. Aprimorar o arcabouço legal sobre segurança cibernética*" e "*2.3.10. Elevar o nível de maturidade da sociedade em segurança cibernética*".

Cumpre referir ainda que a responsabilidade do governo brasileiro quanto à segurança de seus aplicativos móveis não está apenas relacionada à proteção da privacidade de seus cidadãos, mas também à proteção da nação contra ameaças no domínio cibernético.

5.3 RECOMENDAÇÕES AOS USUÁRIOS DOS APLICATIVOS MÓVEIS

Considerando as vulnerabilidades identificadas nos aplicativos móveis do governo brasileiro, apresentadas no Capítulo 4, e o comportamento inseguro de muitos usuários no uso de seus dispositivos, conforme visto no Capítulo 2, esta seção fornece algumas recomendações importantes aos usuários de aplicativos móveis.

Importante destacar que mesmo que os desenvolvedores de aplicativos adotem métodos seguros de desenvolvimento, estes por si só não são suficientes para proteger os usuários, sendo necessário considerar o comportamento individual dos usuários. Portanto, há necessidade de se estabelecer diretrizes para os usuários manterem seus dispositivos móveis seguros e evitar que comprometam desnecessariamente sua privacidade. Neste sentido, este estudo propõe as seguintes recomendações:

R1 - Proteger o acesso ao dispositivo

O nível mais básico de proteção que se deve ter em um dispositivo móvel é o bloqueio de tela. O usuário deve certificar-se de que o dispositivo seja bloqueado automaticamente e tenha uma senha forte, caso contrário, qualquer pessoa pode acessar os dados pessoais do usuário, incluindo os dados de aplicativos de governo, que podem conter informações altamente sensíveis.

Senhas compostas por nomes, apelidos, nomes de animais de estimação, datas de nascimento, números de telefones e documentos são vulneráveis e não devem ser utilizadas. A escolha de um padrão geométrico de desbloqueio de tela deve ser complexo o suficiente para ser seguro, ao invés de fácil e prático. O uso de recursos de desbloqueio biométrico, como impressão digital, são mais recomendados, pois oferecem uma maneira de desbloquear dispositivos móveis mais conveniente (não havendo a necessidade de memorizar códigos secretos) e segura (mais difícil de ser roubada), se comparada à utilização de senhas e padrões geométricos de desbloqueio.

Quando utilizarem senhas e padrões geométricos de desbloqueio, os usuário devem estar atentos a técnica de engenharia social chamada "Shoulder surfing", na qual um adversário observa as teclas digitadas no dispositivo pelo usuário, olhando por cima do seu ombro.

R2 - Garantir que o sistema operacional e aplicativos estejam atualizados

Os usuários devem garantir que o sistema operacional móvel e os aplicativos estejam executando suas versões mais recentes. A execução de sistema operacional e aplicativos mais recentes garante que os dispositivos se beneficiem das melhorias de segurança implementadas pelos desenvolvedores, fornecendo resiliência contra vulnerabilidades que podem ainda não ser conhecidas publicamente.

R3 - Evitar conectar-se a redes Wi-Fi públicas

As redes Wi-Fi públicas fornecem uma maneira conveniente e econômica de acessar a Internet, já que estão cada vez mais disponíveis, em restaurantes, shoppings, academias, mercados e em diversos outros locais. No entanto, é importante que os usuários sejam cautelosos quanto ao uso de redes Wi-Fi públicas, pois são redes inseguras e suscetíveis a uma série de riscos.

Se a conexão for realmente necessária, é aconselhado evitar a utilização de aplicativos que manipulem dados sensíveis do usuário. Configurar uma VPN (Rede Privada Virtual) é altamente recomendável, uma vez que não é possível que o usuário verifique facilmente se um aplicativo trafega dados pela rede de forma segura (criptografada).

R4 - Instalar aplicativos de fontes confiáveis

Aplicativos potencialmente prejudiciais (*malwares*) são importantes ameaças para os usuários do Android e as lojas de aplicativos de terceiros (não oficiais) são as principais portadoras desses aplicativos maliciosos. Portanto, é fundamental que os usuários façam o download de aplicativos apenas de fontes confiáveis, como as lojas oficiais de aplicativos da plataforma. No caso do Android, a Google Play Store é a loja oficial de aplicativos. Em suas lojas oficiais as empresas monitoram os aplicativos disponibilizados para download, verificando sua conformidade com lista extensa de requisitos e, em caso de violação, o aplicativo é banido da loja. Deste modo, os usuários têm maior segurança na instalação de um aplicativo.

Tratando-se de aplicativos móveis do governo brasileiro, além de buscar o aplicativo na loja oficial da plataforma, o usuário deve verificar se o aplicativo é disponibilizado na conta oficial do governo brasileiro. Devido a Portaria nº 39, de 09/07/2019, do Ministério da Economia, os aplicativos governamentais são disponibilizados por meio de uma conta única do Governo Federal.

R5 - Evitar o *rooting* do dispositivo

A obtenção de direitos de acesso de superusuário, popularmente conhecido como *root*, permite que os proprietários assumam o controle total de seus dispositivos e os motivos mais comuns são para obter acesso irrestrito ao sistema, melhorar o desempenho do dispositivo, instalar diferentes versões do sistema operacional, entre outros. Porém, essa prática não é recomendada pois viola importantes mecanismos de segurança, deixando o sistema mais vulnerável a *malware* e outras ameaças.

R6 - Desativar recursos não utilizados

É importante ainda que os usuários de dispositivos móveis desativem todos os recursos que não estão em uso no momento, reduzindo assim a superfície de ataque. Uma prática recomendada é desligar o Wi-Fi quando ele não estiver sendo usado, isso impedirá que o dispositivo procure por um ponto de acesso próximo e se conecte a ele sem a verificação do usuário. É recomendável ainda desativar outros recursos que não estiverem em uso, como: Bluetooth, GPS, NFC, entre outros.

R7 - Remover aplicativos não utilizados

Um software desatualizado ou que foi desenvolvido sem níveis adequados de segurança pode se tornar um potencial ponto de vulnerabilidade. Dessa forma, se um aplicativo está sem uso há muito tempo, deve-se avaliar a possibilidade de removê-lo. A simples remoção de aplicativos antigos desnecessários pode ajudar a tornar o dispositivo muito mais seguro.

R8 - Ser cuidadoso ao utilizar estações de carregamento em áreas públicas

O uso intenso de dispositivos móveis faz com que os usuários precisem frequentemente carregar seus dispositivos. Diante disso, cresceu o número de locais públicos que oferecem estações de carregamento, por exemplo, em shoppings, aeroportos e terminais de ônibus.

A interface USB é utilizada pelos dispositivos móveis tanto para carregamento como para transferência de dados, dessa forma, se um dispositivo estiver conectado a uma estação de carregamento maliciosa, a estação pode explorar vulnerabilidades nesse canal de comunicação para obter dados confidenciais do usuário.

Portanto, os usuários devem ser cautelosos ao utilizarem estações públicas de carregamento, não fazendo a carga do dispositivo por meio de conexão USB, em vez disso, utilizar diretamente uma tomada elétrica, preferencialmente, utilizando cabos e carregadores originais do dispositivo, uma vez que há histórico de carregadores não originais desenvolvidos não apenas para carregamento, mas também para coleta de dados do dispositivo.

R9 - Avaliar atentamente as permissões de aplicativos

As permissões do Android são um importante mecanismo para proteger os recursos do sistema e a privacidade dos usuários, tendo os usuários um papel fundamental na aplicação dessas permissões. Como visto, os aplicativos costumam exigir mais permissões do que o necessário. Portanto, os usuários podem evitar problemas de segurança e privacidade revisando o escopo de permissões solicitadas pelos aplicativos instalados no dispositivo. Caso as permissões solicitadas não sejam compatíveis com as funções descritas, a permissão pode ser removida ou o aplicativo desinstalado.

R10 - Estabelecer procedimentos de emergência e descarte

É importante que os usuários tenham em mente os procedimentos a serem seguidos em caso de emergência (roubo/furto do dispositivo) e descarte do dispositivo. Caso o usuário acredite que o dispositivo possa ter caído em mãos erradas, é fundamental ter o número de série e os números IMEI do dispositivo, para solicitar o bloqueio junto a operadora de telefonia e para notificar as autoridades locais. Além disso, é recomendado que o usuário tenha habilitado funções de localização e apagamento remoto, impossibilitando que um adversário mal intencionado tenha acesso a dados confidenciais do usuário.

Em caso de descarte, devido ao dispositivo não ter mais uso para o usuário, é imprescindível que o usuário faça a exclusão dos dados do dispositivo de forma segura, realizando o procedimento chamado "Data Wiping", que não permite a recuperação dos dados apagados.

Caso os usuários adotem as recomendações propostas neste estudo, eles estarão menos suscetíveis às vulnerabilidades identificadas nos aplicativos móveis do governo brasileiro. Na Seção 2.6 são apresentadas algumas possíveis ameaças aos usuários, as quais são mitigadas pelas recomendações propostas neste estudo, conforme tabela 5.1.

Tabela 5.1: Mitigação das ameaças de adversários por meio de recomendações aos usuários.

		Ameças de Adversários			
		AD01: Adversário com acesso físico ao dispositivo	AD02: Estação Maliciosa com Acesso Físico ao Dispositivo	AD03: Aplicativo Malicioso	AD04: Adversário de Rede
Recomendação ao Usuário	R1 - Proteger o acesso ao dispositivo	●	●		
	R2 - Garantir que o sistema operacional e aplicativos estejam atualizados	◒	◒	◒	◒
	R3 - Evitar conectar-se a redes Wi-Fi públicas				●
	R4 - Instalar aplicativos de fontes confiáveis			●	◒
	R5 - Evitar o rooting do dispositivo	◒	◒	●	●
	R6 - Desativar recursos não utilizados			◒	●
	R7 - Remover aplicativos não utilizados			◒	◒
	R8 - Ser cuidadoso ao utilizar estações de carregamento em áreas públicas		●		
	R9 - Avaliar atentamente as permissões de aplicativos			◒	
	R10 - Estabelecer procedimentos de emergência e descarte	●	●	●	●

(Sem ícone) Não previne ● Previne frequentemente ◒ Previne algumas vezes

5.4 PRINCIPAIS CONTRIBUIÇÕES DA PESQUISA

A principal contribuição do presente trabalho é que, diferentemente dos trabalhos anteriores que se concentram mormente em aplicativos comerciais, o foco desta dissertação é na análise de aplicativos móveis do governo brasileiro, fornecendo as seguintes colaborações:

1. Avaliamos o estado de segurança e privacidade de trinta aplicativos móveis do governo brasileiro, que totalizam mais de 93,5 milhões de downloads e representam mais de 95,8% dos downloads da loja oficial do governo federal;

2. Apresentamos de forma detalhada os principais pontos vulneráveis dos aplicativos móveis do governo brasileiro e, principalmente, quais dados dos usuários e dos aplicativos podem ser comprometidos;

3. Contribuímos, através dos resultados da pesquisa e das recomendações à Administração Pública e ao cidadão, para a construção de um país onde os dados pessoais são devidamente protegidos e a privacidade do cidadão é respeitada.

4. Apresentamos um modelo de ameaças e cenários de ataque para aplicativos móveis, colaborando para a evolução do conhecimento de análise de segurança de aplicativos móveis;

5.5 TRABALHOS FUTUROS

Há diversas possibilidades para trabalhos futuros. Eis algumas:

1. Reavaliar os aplicativos, quanto aos critérios estabelecidos neste estudo, a fim de verificar se as vulnerabilidades notificadas aos desenvolvedores foram corrigidas;

2. Avaliar a segurança e a privacidade dos aplicativos móveis do governo brasileiro para a plataforma *iOS*, da empresa *Apple*, segundo os critérios mínimos estabelecidos na Seção 3.2;

3. Avaliar a adequação dos aplicativos móveis do governo brasileiro e de suas políticas de privacidade quanto à Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018.

4. Avaliar a conformidade dos aplicativos móveis do governo brasileiro com os requisitos estabelecidos no "OWASP Mobile Application Security Verification Standard (MASVS)"(Mueller et al., 2022), para uma verificação mais abrangente.

REFERÊNCIAS

Andriotis, P., Oikonomou, G., Mylonas, A. e Tryfonas, T. (2016). A study on usability and security features of the android pattern lock screen. *Inf. Comput. Secur.*, 24:53–72.

Android Developers (2020). Android debug bridge (adb). `https://developer.android.com/studio/command-line/adb`. Acessado em 20/06/2022.

Android Developers (2021). Permissões no android. `https://developer.android.com/guide/topics/permissions/overview`. Acessado em 20/06/2022.

Apktool (2020). Apktool. `https://ibotpeaches.github.io/Apktool/`. Acessado em 20/06/2022.

AVAST (2018). 95% dos brasileiros estão usando senhas fracas. `https://press.avast.com/pt-br/95-dos-brasileiros-estao-usando-senhas-fracas`. Acessado em 20/06/2022.

Bergadano, F., Boetti, M., Cogno, F., Costamagna, V., Leone, M. e Evangelisti, M. (2020). A modular framework for mobile security analysis. *Information Security Journal: A Global Perspective*, 29:220 – 243.

Botacin, M., Kalysch, A. e Grégio, A. (2019). The internet banking [in]security spiral: Past, present, and future of online banking protection mechanisms based on a brazilian case study. *Proceedings of the 14th International Conference on Availability, Reliability and Security*.

Breitinger, F., Tully-Doyle, R. e Hassenfeldt, C. (2020). A survey on smartphone user's security choices, awareness and education. *Comput. Secur.*, 88.

Casati, L. e Visconti, A. (2018). The dangers of rooting: Data leakage detection in android applications. *Mob. Inf. Syst.*, 2018:6020461:1–6020461:9.

Comitê Gestor da Internet do Brasil - CGI.br (2019). Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: Tic domicílios 2019. `https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2019/`. Acessado em 20/06/2022.

Croft, R., Newlands, D., Chen, Z. e Babar, M. A. (2021). An empirical study of rule-based and learning-based approaches for static application security testing. *Proceedings of the 15th ACM / IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*.

Dalvi, T. e Trummer, T. (2015). QARK: Android App Exploit and SCA Tool. *AppSecUSA 2015*.

Dalziel, H. e Abraham, A. (2016). Automated Security Analysis of Android and iOS Applications with Mobile Security Framework. *Network Security*.

Decreto nº 10.222, de 5 de fevereiro de 2020 (2020). Aprova a Estratégia Nacional de Segurança Cibernética. Diário Oficial da União, Brasília, DF, 06/02/2020. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acessado em 20/06/2022.

Deliberação Contran nº 180, de 30 de dezembro de 2019 (2019). Dispõe sobre os requisitos para emissão do Certificado de Registro e Licenciamento de Veículo em meio eletrônico (CRLV-e). Diário Oficial da União, Brasília, DF, 31/12/2019. https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2019/. Acessado em 20/06/2022.

Denning, P. J. (1968). The working set model for program.

Elenkov, N. (2021). Android Backup Extractor. https://github.com/nelenkov/android-backup-extractor. Acessado em 20/06/2022.

European Union Agency For Network and Information Security (2018). Privacy and data protection in mobile applications : a study on the app development ecosystem and the technical implementation of gdpr. https://data.europa.eu/doi/10.2824/114584. Acessado em 20/06/2022.

Exodus Privacy (2021). Trackers. https://reports.exodus-privacy.eu.org/en/info/trackers/. Acessado em 20/06/2022.

Franklin, J., Brown, C., Dog, S. E., McNab, N., Voss-Northrop, S., Peck, M. A. e Stidham, B. (2016). Assessing threats to mobile devices & infrastructure: the mobile threat catalogue. Em *NISTIR 8144*.

Ganapati, S. (2015). Using mobile apps in government. *Washington DC: IBM Center for The Business of Government*.

Gil, C., Baquero Rey, L. e Hernandez Bejarano, M. (2018). A conceptual exploration for the safe development of mobile devices software based on owasp. *International Journal of Applied Engineering Research*, 13:13603–13609.

Google e Brain & Company (2020). Impacto econômico e social do android no brasil. https://www.bain.com/contentassets/20e0815cfd784b4a8dead63475b42380/v02_b-impactos-do-android-no-brasil.pdf. Acessado em 20/06/2022.

Gordon, M. I., Kim, D., Perkins, J. H., Gilham, L., Nguyen, N. e Rinard, M. C. (2015). Information Flow Analysis of Android Applications in DroidSafe. Em *Network and Distributed System Security (NDSS)*.

Governo do Brasil (2017). Manual de Elaboração de Atos Normativos no Ministério da Justiça e Segurança Pública. https://www.gov.br/mj/pt-br/assuntos/seus-direitos/elaboracao-legislativa/manual_elaboracao_atos_normativos_mjsp-portaria-gm-n-776-de-5-de-setem.pdf. Acessado em 20/06/2022.

Governo do Brasil (2021a). Guia de Boas Práticas - Lei Geral de Proteção de Dados Pessoais (LGPD). https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf/view. Acessado em 20/06/2022.

Governo do Brasil (2021b). Guia de Requisitos Mínimos de Segurança e Privacidade para Aplicativos Móveis. https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_seguranca_apps.pdf/view. Acessado em 20/06/2022.

Hazum, A., Danin, A., Melnykov, B., Tsymberg, D. e Wernik, I. (2021). Mobile app developers' misconfiguration of third party services leave personal data of over 100 million exposed. https://research.checkpoint.com/2021/mobile-app-developers-misconfiguration-of-third-party-services-leave-personal-data-of-over-100-million-exposed/. Acessado em 20/06/2022.

Kaspersky Lab (2017). Rooting your Android: advantages, disadvantages, and snags. https://www.kaspersky.com/blog/android-root-faq/17135/. Acessado em 20/06/2022.

Kesäniemi, A. e Mäkelä, J. (2011). Mobile Application Threat Analysis. OWASP Helsinki Chapter Meeting #15. https://owasp.org/www-pdf-archive/Mobile-threat-analysis-short-presentation_owasp.pdf. Acessado em 20/06/2022.

Knopp, M. (2005). Mobile government in germany: Legal aspects and demands on mobilizing the administration.

Kohli, N. e Mohaghegh, M. (2020). Security testing of android based covid tracer applications. *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, páginas 1–6.

Lei 13.709, de 14 de agosto de 2018 (2018). Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15/08/2018. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acessado em 20/06/2022.

Lei 9.609, de 19 de fevereiro de 1998 (1998). Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Diário Oficial da União, Brasília, DF, 20/02/1998. http://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acessado em 20/06/2022.

Lei 9.610, de 19 de fevereiro de 1998 (1998). Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Diário Oficial da União, Brasília, DF, 20/02/1998. http://www.planalto.gov.br/ccivil_03/leis/l9610.htm. Acessado em 20/06/2022.

Lero, A. R. S., Lero, J. B. e Gear, A. L. (2019). Privacy and security analysis of cryptocurrency mobile applications. *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)*, páginas 1–6.

Lin, Y. (2015). AndroBugs Framework: An Android Application Security Vulnerability Scanner. https://www.blackhat.com/docs/eu-15/materials/eu-15-Lin-Androbugs-Framework-An-Android-Application-Security-Vulnerability-Scanner.pdf. Acessado em 20/06/2022.

Los Angeles County District Attorney's Office (2019). Fraud Alerts: "Juice Jacking" Criminals Use Public USB Chargers to Steal Data. http://da.lacounty.gov/community/fraud-alerts/juice-jacking-criminals-use-public-usb-chargers-steal-data. Acessado em 20/06/2022.

Maro, E. e Kovalchuk, M. (2018). Bypass biometric lock systems with gelatin artificial fingerprint. Association for Computing Machinery.

MITRE Corporation (2022). CWE-295: Improper Certificate Validation. https://cwe.mitre.org/data/definitions/295.html. Acessado em 20/06/2022.

Mobile Time e Opinion Box (2020). Roubos de Celulares no Brasil - Julho/2020. https://www.mobiletime.com.br/pesquisas/celulares-roubados-julho-de-2020/. Acessado em 20/06/2022.

Mueller, B., Schleier, S., Willemsen, J. e Holguera, C. (2020). OWASP Mobile Security Testing Guide . https://owasp.org/www-project-mobile-security-testing-guide/. Acessado em 20/06/2022.

Mueller, B., Schleier, S., Willemsen, J. e Holguera, C. (2022). OWASP Mobile Application Security Verification Standard (MASVS). https://github.com/OWASP/owasp-masvs. Acessado em 20/06/2022.

Negi, C., Mishra, P., Chaudhary, P. e Vardhan, H. (2021). A review and case study on android malware: Threat model, attacks, techniques and tools. *J. Cyber Secur. Mobil.*, 10:231–260.

Neto, E. O. M. (2020). *Governo móvel no Brasil: uma análise do estado da arte no desenvolvimento de aplicativos móveis por instituições do setor público brasileiro.* Tese de doutorado, Universidade Federal da Bahia.

Norton (2017). Norton Wi-Fi Risk Report. https://www.nortonlifelock.com/us/en/newsroom/press-kits/norton-wifi-risk-report-2017/. Acessado em 20/06/2022.

Osho, O., Mohammed, U. L., Nimzing, N. N., Uduimoh, A. A. e Misra, S. (2019). Forensic analysis of mobile banking apps. Em *International Conference on Computacional Science an Its Applications (pp. 613-626).*

Oui-Suk, U. (2010). Introduction of m-Government & IT Convergence Technology.

OWASP (2016). OWASP Mobile Top Ten 2016. https://owasp.org/www-project-mobile-top-10/. Acessado em 20/06/2022.

Paulsen, C. e Byers, R. (2019). NIST7298 - Glossary of key information security terms. https://doi.org/10.6028/nist.ir.7298r3. Acessado em 20/06/2022.

Phumkaew, N. e Visoottiviseth, V. (2018). Android forensic and security assessment for hospital and stock-and-trade applications in thailand. *2018 15th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, páginas 1–6.

Portaria nº 39, de 09 de julho de 2019 (2019). Dispõe sobre procedimentos para a unificação dos canais digitais e define regras para o procedimento de registro de endereços de sítios eletrônicos na internet e de aplicativos móveis do Governo Federal. Diário Oficial da União, Brasília, DF, 11/07/2019. https://www.in.gov.br/en/web/dou/-/portaria-n-39-de-9-de-julho-de-2019-191674589. Acessado em 20/06/2022.

Ravnas, O. A. V. (2022). Frida. https://frida.re/. Acessado em 20/06/2022.

Reed, B. (2019). NowSecure: Test of 250 Popular Android Mobile Apps Reveals that 70% Leak Sensitive Personal Data. https://www.nowsecure.com/blog/2019/06/06/test-of-250-popular-android-mobile-apps-reveal-that-70-leak-sensitive-personal-data/. Acessado em 20/06/2022.

Samsung (2019). 10 essential tips to keep your mobile device secure. https://www.samsung.com/us/business/short-form/keep-your-personal-and-work-mobile-data-safe. Acessado em 20/06/2022.

Souppaya, M. e Scarfone, K. (2013). Guidelines for Managing the Security of Mobile Devices in the Enterprise. Special Publication (NIST SP), National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-124r1. Acessado em 20/06/2022.

Statcounter (2020). Mobile operating system market share brazil - 2020. https://gs.statcounter.com/os-market-share/mobile/brazil/2020. Acessado em 20/06/2022.

Stylios, I. C., Kokolakis, S., Thanou, O. e Chatzis, S. P. (2016). Users' attitudes on mobile devices: Can users' practices protect their sensitive data? Em *MCIS*.

Sun, R., Wang, W., Xue, M., Tyson, G., Çamtepe, S. e Ranasinghe, D. (2021). An empirical assessment of global covid-19 contact tracing applications. *2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE)*, páginas 1085–1097.

Supremo Tribunal Federal (2021). Lei Geral de Proteção de Dados Pessoais (LGPD). https://www.stj.jus.br/sites/portalp/Leis-e-normas/lei-geral-de-protecao-de-dados-pessoais-lgpd. Acessado em 20/06/2022.

Tarandach, I. e Coles, M. (2020). *Threat Modeling: A Practical Guide for Development Teams*. O'Reilly Media, Incorporated.

U.S. Department of Homeland Security - DHS (2017). Study on mobile device security. https://www.dhs.gov/publication/st-mobile-device-security-study?topic=cybersecurity. Acessado em 20/06/2022.

Velu, V. K. (2016). *Mobile Application Penetration Testing*. Packt Publishing.

Wang, Z. e Stavrou, A. (2010). Exploiting smart-phone usb connectivity for fun and profit. Em *ACSAC '10*.

APÊNDICE A – RELATÓRIO DETALHADO DE ANÁLISE

Este Apêndice apresenta brevemente os aplicativos selecionados na Seção 3.1 e suas principais funcionalidades. Cada aplicativo é analisado a partir dos critérios de segurança e privacidade estabelecidos na Seção 3.2 e os resultados são abordados em detalhes. Algumas descobertas são semelhantes entre os aplicativos, no entanto, elas foram mantidas por ainda serem relevantes para a aplicação em questão. No Capítulo 4, apresentamos uma discussão a respeito dos resultados do experimento.

Este Apêndice será mantido em sigilo por um prazo definido, conforme esclarecido na Seção 1.4.