José Lucio C. Azevedo

Cibersegurança em Aplicações Bancárias no Android: Um artigo de revisão sobre pontos críticos e métodos de segurança

Campos dos Goytacazes, RJ

25 de junho de 2024

José Lucio C. Azevedo

Cibersegurança em Aplicações Bancárias no Android: Um artigo de revisão sobre pontos críticos e métodos de segurança

Projeto de pesquisa apresentado como requisito para aprovar a disciplina de Projeto de Monografia do Curso de Bacharel em Ciência da Computação, da Universidade Estadual do Norte Fluminense Darcy Ribeiro

Universidade Estadual do Norte Fluminense Darcy Ribeyro

CCT - Laboratório de Ciencias Matemáticas

Curso de Ciência da Computação

Campos dos Goytacazes, RJ

25 de junho de 2024

Lista de ilustrações

Sumário

Capítulo 1:
Introdução

Desde os tempos antigos os métodos de pagamento e manipulação de dinheiro vem mudando de maneira constante. Segundo Téllez e Zeadally (2017), antes de haver um sistema monetário o pagamento era feito com trocas de mercadoria e isso foi eficiente enquanto as necessidades humanas eram limitadas. Entretanto, com o crescimento da complexidade da sociedade, este método se tornou insuficiente e o homem teve que adotar outros sistemas como moedas de minério, e após isso, dinheiro e o cartão bancário. Com o avanço tecnologico, rápido desenvolvimento da tecnologia de redes móveis e os avanços nos dispositivos portáteis, tornou-se possível que as pessoas acessassem a Internet usando dispositivos móveis em qualquer lugar e a qualquer hora para realizar transações de comércio eletrônico e outras operações, como navegação na web, leitura de e-mail e assim por diante. Dessa forma, foi possível a criação de novos métodos práticos, fáceis e rápidos de pagamento e manipulação de dinheiro.

O banco móvel, segundo Singhal, Nath e Goel (2019), se refere à provisão de serviços bancários, tais como transferências, verificação de saldos, efetuação de pagamentos, investimentos e outras transações, através de dispositivos portáteis que suportam aplicativos. Essencialmente, mencionando dispositivos como smartphones, tablets e, em alguns casos, smartwatches. Com essa capacidade, os clientes têm à disposição a maioria dos serviços oferecidos por suas instituições financeiras na palma de suas mãos, sem a necessidade de visitar uma agência bancária ou um caixa eletrônico, nem de estar em frente a um computador de mesa ou laptop.

As estatísticas confirmam (DELOITTE, 2021) que a adoção dessa abordagem de interação com as instituições financeiras está ganhando força. Na imagem 1 pode-se observar alguns exemplos de aplicações bancárias brasileiras.

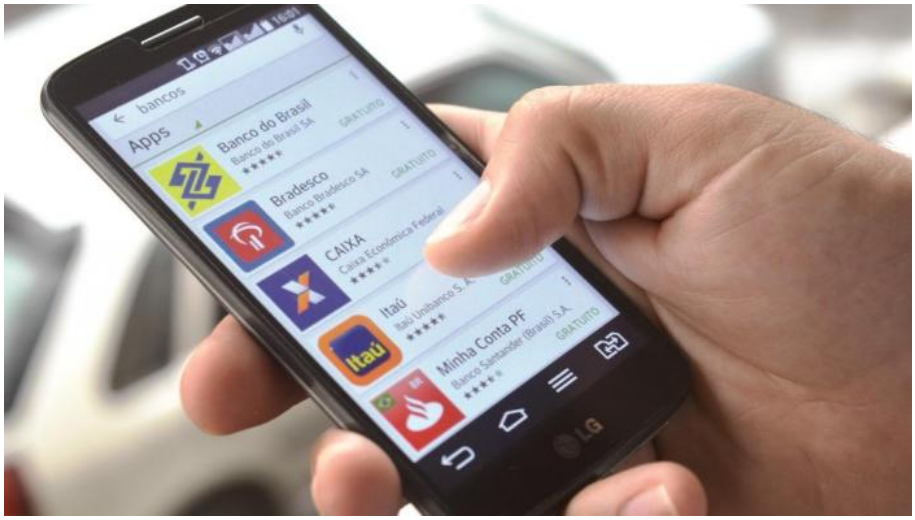

Figura 1 – Aplicações de banco móvel

Uma pesquisa encomendada pela Federação Brasileira de Bancos e realizada pela empresa Deloitte (2021) sobre tecnologia bancária revelou um aumento de 20% no número de transações realizadas por dispositivos móveis de 2019 para 2020. Enquanto em 2019 foram efetuadas 37 bilhões de transações, no ano seguinte esse número saltou para 52,9 bilhões. Esse crescimento foi impulsionado pela pandemia e pelo programa de auxílio emergencial e essa combinação de fatores consolidou os celulares e outros dispositivos móveis como um dos principais canais de atendimento no setor bancário, como analisado na imagem 2.

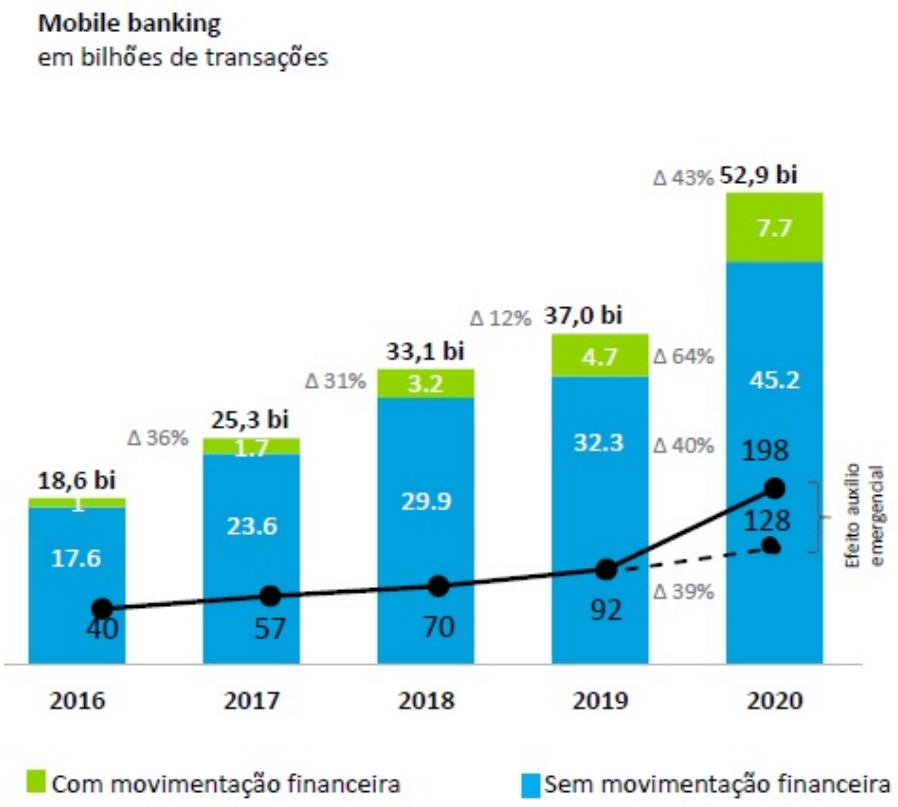

Figura 2 – Número de transações mobile

Fonte: (DELOITTE, 2021)

Nesse sentido, a segurança da informação desempenha um papel fundamental no contexto das aplicações bancárias móveis. Dada a crescente popularidade destas tecnologias, é importante garantir que os dados sensíveis dos utilizadores sejam protegidos. As transações financeiras e o acesso a informações pessoais estão em risco, e as violações de segurança podem ter consequências graves, como roubo financeiro, fraude e até mesmo comprometimento da identidade do usuário. Portanto, investir em medidas de segurança robustas não apenas tranquilizará seus clientes, mas também aumentará sua confiança ao usar esses aplicativos. A segurança da informação não é apenas uma prioridade, mas também necessária para que os pagamentos móveis e os serviços bancários móveis continuem a evoluir e a beneficiar os consumidores de uma forma segura e eficaz. Para fazer esses aplicativos seguros é importante entender os problemas de segurança que ele traz, como por exemplo dispositivos perdidos, riscos na rede, senhas fracas, vazamentos e erros humanos. Muitas vezes existe a implementação indevida dessa ferramenta que abre brechas para atacantes, e como esse tipo de aplicativo lida diretamente com o dinheiro, eles mais do que qualquer outro tem que ter a segurança impecável e lidar com esses problemas citados.

Em 2015, dois pesquisadores, Aranha e Cruz (2015), da Unicamp realizaram um

estudo para identificar deficiências e fragilidades nos aplicativos de alguns bancos gigantes brasileiros para android e o resultado foi no mínimo problemático. Como mostrado na Figura 3, foi descoberto que alguns desses aplicativos utilizavam métodos extremamente básicos de segurança e muitas vezes sabidamente vulneráveis a ataques de segurança simples, como ataques de interceptação de dados e vazamento de dados. Foram dadas notas que variam de 0 a 5 estrelas para as aplicações.

	Banco do Brasil	Bradesco	Caixa Econômica Federal	Citibank	HSBC	Itaú	Santander
Vazamento de credenciais	✘	✔	✔	✔	✘	✔	✔
MITM	✘	✘	✘	✘	✘	✘	✔
MITM com certificado raiz	✘	✔	✔	✔	✔	✔	✔
Redes sociais externas	✘	✔	✘	✔	✘	✔	✘
Ausência de pinagem	✘	✔	✔	✔	✔	✔	✔
Nota	★★★★★	★★	★★½	★★	★★★½	★★	½

Figura 3 – Resultado dos aplicativos Android analisados

Fonte: (ARANHA; CRUZ, 2015)

Somado a isso, como dito por Wang, Hahn e Sutrave (2016), os ataques de hackers a aplicações e serviços bancários são uma ameaça crescente e significativa no mundo digital. À medida que o uso dessas tecnologias aumenta, os cibercriminosos exploram vulnerabilidades para obter acesso às informações financeiras confidenciais dos usuários e estão constantemente desenvolvendo estratégias avançadas.

A todo instante são estudadas formas de desenvolver aplicações cada vez mais seguras e blindadas de ataques, identificar vulnerabilidade e propor correções antes de serem encontradas por algum indivíduo de fato malicioso. Entretanto, as aplicações bancárias incorporam características específicas, descritas em Islam (2014), e para garantir a segurança da informação em um cenário digital é cada vez mais complexo.

1.1 Problemática

As aplicações bancárias são alvos atraentes para cibercriminosos devido à quantidade significativa de informações sensíveis que manipulam, incluindo dados pessoais, credenciais de acesso e informações financeiras. A complexidade do ecossistema móvel, combinada com práticas inadequadas de desenvolvimento e a crescente sofisticação dos ataques cibernéticos, aumenta a probabilidade de vulnerabilidades exploráveis. Tais vulnerabilidades podem resultar em ataques e outras formas de exploração que comprometem a segurança dos usuários e das instituições financeiras.

A diversidade áreas, métodos e práticas de segurança tornam difícil estabelecer diretrizes comuns e mais críticas levando em consideração as características específicas

das aplicações financeiras, que não são completamente supridas pelos métodos atuais utilizados em outros tipos de aplicações, criando uma lacuna potencial na proteção dos dados e recursos dos usuários.

1.2 Hipótese

A criação de um modelo de segurança eficaz, abrangente e específico para aplicações bancárias móveis podem estabelecer diretrizes claras para o desenvolvimento seguro, abordando aspectos e cenários específicos do meio financeiro digital, e alcançar o conhecimento dos pontos críticos e por conseguinte métodos se segurança consistentes e resistentes a ataques.

1.3 Objetivos

O objetivo geral desse presente trabalho é aprimorar a segurança dessas plataformas, promovendo a confidencialidade, integridade e disponibilidade das aplicações bancárias no Android, bem como contribuir para a compreensão aprofundada das melhores práticas e métodos de segurança adaptadas a este cenário específico.

Os objetivos específicos incluem:

- Pesquisa: Realizar uma pesquisa visando entender, selecionar e desmistificar os principais pontos críticos de segurança em aplicações bancárias móvel e suas remediações.
- Criação: Propor, como conclusão de uma revisão bibliográfica, tópicos que devem ser tratados como prioridade na implementação desse tipo de aplicação, seus conceitos e breves implementações.

1.4 Justificativa

A crescente popularidade de sistemas de pagamento móvel tornou aplicações de pagamento e banco móvel alvos atrativos para cibercriminosos, e, consequentemente, a necessidade de uma padrão de segurança simples e específico para a implementação da segurança dessas aplicações específicas é evidente.

Através da desmistificação da segurança da informação, é necessário fortalecer a resiliência desses sistemas em um ambiente digital em constante evolução, garantindo a

confiança dos usuários e instituições financeiras no uso seguro de dispositivos de pagamento móvel e banco móvel.

1.5 Resultados esperados

Com a conclusão deste estudo, espera-se obter uma compreensão aprofundada dos aspectos críticos de cibersegurança em aplicações bancárias no sistema operacional Android, isso é, um conhecimento abrangente das principais ameaças e vulnerabilidades que afetam as aplicações bancárias no Android, com base na análise de literatura existente. Além disso fornecer um conjunto claro de melhores práticas e recomendações para desenvolvedores de aplicações bancárias. E com isso, a divulgação de conhecimentos sobre as ameaças e as medidas de mitigação contribuirá para uma cultura de segurança mais sólida no desenvolvimento de software.

Capítulo 2:
Base teórica

2.1 Segurança da informação

Segurança da informação é o conjunto de práticas, políticas, procedimentos e tecnologias que tem como objetivo proteger as informações de uma organização. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

Para implementar aplicações seguras, Hintzbergen et al. (2018) descreve que é necessário implementar um conjunto adequado de controles, políticas, processos, procedimentos, estruturas e funções tanto de software, quanto de hardware. Existe a necessidade de estabelecer, implementar, monitorar, revisar e melhorar onde necessário, para ter certeza que os objetivos específicos da segurança da informação estão sendo atendidos. Esse objetivo é manter os pilares principais da segurança da informação, que são a confidencialidade, integridade e disponibilidade. Mas também é importante citar a autenticidade e o não-repúdio.

2.1.1 Confidencialidade

A confidencialidade, segundo Hintzbergen et al. (2018), se refere aos limites em termos de quem pode obter que tipo de informação, isso é, o ato de garantir que a informação seja acessível apenas àqueles autorizados a ter acesso. Nomes, CPFs, números de cartão, transações e registros financeiros, entre outras informações sensíveis, devem ter acesso autorizado somente aos indivíduos com permissão para ver tal informação.

A confidencialidade, segundo Hintzbergen et al. (2018), garante que o nível necessário de sigilo seja aplicado em cada elemento de processamento de dados e impede a divulgação não autorizada. Esse nível de confidencialidade deve prevalecer enquanto os dados residirem em sistemas e dispositivos na rede, quando forem transmitidos e quando

chegarem ao seu destino.

Este pilar pode ser fornecida através da criptografia de dados à medida que são armazenados e transmitidos, usando preenchimento de tráfego na rede, estrito controle de acesso, classificação dos dados e treinamento de pessoal nos procedimentos apropriados.

2.1.2 Integridade

A integridade, segundo Hintzbergen et al. (2018), assegura que os dados utilizados, enviados e armazenados por organizações são confiável e não apagados, danificados ou alterados. Uma informação uma vez armazenada, espera-se que ela se mantenha integra, isso é, correta, autêntica e confiável.

Os dados devem ser protegidos contra exclusão e modificação por parte não autorizada, enquanto estão em uso, em trânsito e quando são armazenados, independentemente de residirem em um laptop, dispositivo de armazenamento, data center ou na nuvem. Mesmo que um indivíduo autorizado fizer alterações por engano, essas alterações devem poder ser revertidas.

2.1.3 Disponibilidade

A disponibilidade, segundo Hintzbergen et al. (2018), refere-se à garantia de que os sistemas e recursos de informação estejam acessíveis sempre que necessários, mesmo diante de eventos adversos, para que os objetivos de negócio e as expectativas dos clientes sejam satisfeitos.

Para manter a disponibilidade, as organizações implementam estratégias de redundância, backups regulares e planos de continuidade de negócios. Essas medidas são cruciais em ambientes nos quais a interrupção dos serviços pode resultar em prejuízos substanciais, como no setor financeiro ou em serviços de emergência. A disponibilidade não apenas implica a prevenção de falhas, mas também a rápida recuperação diante de situações imprevistas, garantindo a continuidade operacional.

2.1.4 Autenticidade

A autenticidade, segundo Hintzbergen et al. (2018), foca na verificação da identidade de usuários, sistemas ou dados. Em transações digitais, a autenticidade é essencial para prevenir acessos não autorizados e estabelecer a confiança nas comunicações. Métodos como senhas, PIN, autenticação de dois fatores e biometria são implementados para garantir que apenas entidades legítimas tenham acesso aos recursos.

A autenticidade é particularmente crítica em setores nos quais a validação da identidade é fundamental, como em sistemas de pagamento online ou em ambientes corporativos que exigem controle de acesso rigoroso.

2.1.5 Não-repúdio

O princípio de não repúdio, segundo Hintzbergen et al. (2018), visa garantir que o autor não negue ter criado e assinado o documento. Ele é vital para garantir que as partes envolvidas em uma transação digital não possam negar sua autoria ou participação. Este pilar é alcançado por meio do uso de assinaturas digitais, registros de auditoria e outros mecanismos que geram evidências irrefutáveis das ações realizadas.

Nos setores legais e financeiros, o não repúdio é essencial para a validação de transações, pagamentos e contratos, garantindo a responsabilidade das partes envolvidas nos processos. Este princípio não apenas reforça a confiabilidade nas interações digitais, mas também contribui para a solução de disputas e questões de conformidade.

2.2 Sistema operacional Android

O Android (LLC, 2024) é um sistema operacional de código aberto baseado no kernel Linux, desenvolvido inicialmente pela Android Inc. e adquirido pelo Google em 2005. Lançado oficialmente em 2008, o Android rapidamente se tornou o sistema operacional móvel dominante no mercado global, sendo utilizado por uma ampla variedade de dispositivos, incluindo smartphones, tablets, smartwatches, televisões e automóveis. A arquitetura do Android é composta por várias camadas, cada uma desempenhando um papel crucial na funcionalidade e segurança do sistema. Essas camadas incluem o kernel do Linux, responsável pela comunicação entre o hardware e o software, gerenciamento de recursos, segurança e drivers de dispositivo; bibliotecas nativas escritas em C/C++ que fornecem suporte para várias funcionalidades, como gráficos, bancos de dados e multimídia; Android Runtime (ART), o runtime que executa aplicações Android e substituiu o Dalvik Virtual Machine, proporcionando melhor desempenho e menor consumo de memória; framework de aplicações, um conjunto de APIs que permite aos desenvolvedores criar aplicações, fornecendo acesso a serviços do sistema como gerenciador de atividades, gerenciador de janelas e provedores de conteúdo; e as aplicações do sistema, que são aplicativos pré-instalados que fornecem funcionalidades básicas como telefone, e-mail, navegador web e contatos.

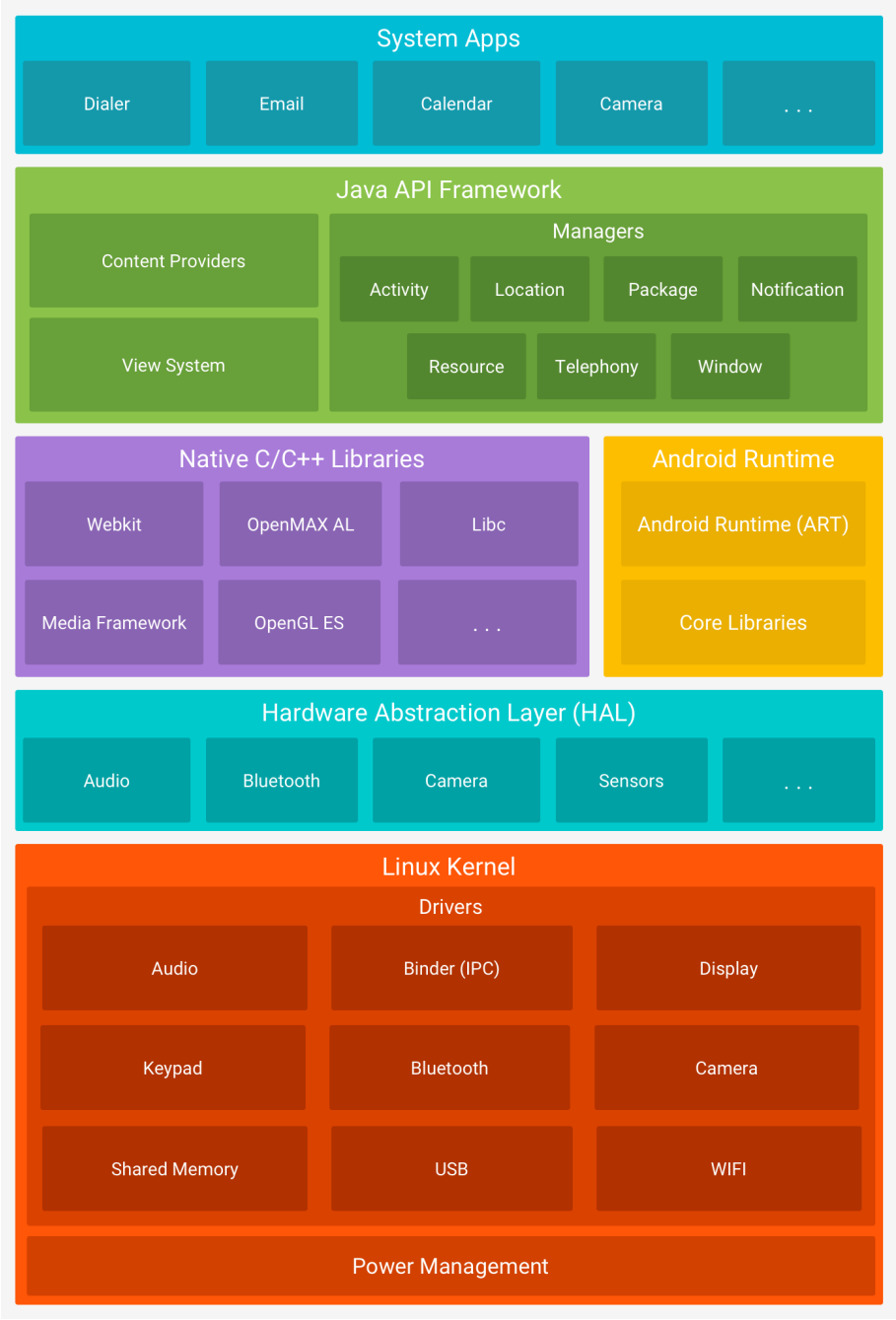

Figura 4 – Arquitetura do Android

O Android incorpora diversos mecanismos de segurança (LLC, 2024) destinados a proteger o sistema e os dados do usuário contra ameaças e ataques. Entre os principais mecanismos estão o modelo de permissões, onde as aplicações devem declarar permissões específicas para acessar recursos protegidos do sistema, e os usuários devem conceder explicitamente essas permissões; sandboxing, que isola cada aplicação em seu próprio ambiente, impedindo o acesso direto aos dados de outras aplicações ou do sistema operacional; assinatura de aplicações, que garante a integridade da aplicação e permite que o sistema identifique a origem do software; atualizações de segurança, lançadas regularmente pelo

Google para corrigir vulnerabilidades identificadas; e o Google Play Protect, um serviço que verifica e monitora aplicações instaladas no dispositivo em busca de comportamentos maliciosos.

Apesar desses robustos mecanismos de segurança, o Android enfrenta vários desafios devido à sua natureza aberta e à fragmentação do ecossistema (LLC, 2024). A diversidade de dispositivos e versões do Android pode dificultar a distribuição uniforme de atualizações de segurança, deixando alguns dispositivos vulneráveis por longos períodos. A abertura do ecossistema permite que desenvolvedores distribuam aplicações fora da Google Play Store, aumentando o risco de instalação de aplicativos maliciosos. Além disso, os fabricantes de dispositivos podem modificar o Android, potencialmente introduzindo novas vulnerabilidades ou dificultando a aplicação de patches de segurança padrão.

2.3 Vulnerabilidades, ameaças, riscos e exposição

Garg e Baliyan (2023) classificam vulnerabilidades como defeitos de segurança suscetíveis a exploração, podendo comprometer os pilares da segurança de um sistema. Estas fragilidades podem se manifestar em diferentes camadas, desde falhas de software até configurações inadequadas e podem ser utilizadas para crimes cibernéticos, para violar a sua privacidade, perturbar a infraestrutura e criar riscos para a segurança nacional. Identificar, corrigir, evitar e principalmente conhecer essas vulnerabilidades é crucial para mitigar riscos e garantir que sistemas permaneçam resilientes diante de potenciais ameaças.

2.3.1 OWASP Mobile Top 10 2023 e ciberataques

O OWASP Mobile Top 10 é uma lista das principais ameaças e vulnerabilidades de segurança encontradas em aplicações móveis. É um guia elaborado pela organização OWASP (2023) e uma referência crucial para desenvolvedores, arquitetos de segurança, pentesters e quaisquer profissional envolvido com segurança ou desenvolvimento de aplicações mobile.

OWASP-2023-Initial Release
M1: Improper Credential Usage
M2: Inadequate Supply Chain Security
M3: Insecure Authentication / Authorization
M4: Insufficient Input/Output Validation
M5: Insecure Communication
M6: Inadequate Privacy Controls
M7: Insufficient Binary Protections
M8: Security Misconfiguration
M9: Insecure Data Storage
M10: Insufficient Cryptography

Figura 5 – Owasp Top Ten 2023

A lista identifica e descreve as vulnerabilidades mais comuns e críticas que são encontradas e exploradas em aplicativos móveis, abrangendo desde questões de autenticação e autorização até problemas relacionados à criptografia e gestão de sessões. O OWASP não apenas destaca os desafios de segurança enfrentados pelas aplicações móveis, mas também orienta a comunidade de desenvolvimento na adoção de boas práticas e na implementação de métodos de segurança eficazes contra estas vulnerabilidades. O guia é atualizado frequentemente, tendo como ultima atualização a de 2023, para acompanhar as mudanças no cenário de ameaças, garantindo que os profissionais estejam sempre atualizados e equipados para enfrentar os desafios emergentes na segurança de aplicações móveis. Segundo a própria organização em (OWASP, 2023), as vulnerabilidades são descritas da seguinte maneira.

2.3.1.1 Uso impróprio de credenciais

O uso impróprio de credenciais é uma vulnerabilidade que ocorre quando as aplicações não gerenciam adequadamente as credenciais do usuário. Um exemplo disso seria um desenvolvedor incluir credenciais de serviço diretamente no código-fonte ou o uso de senhas fracas, tornando-as facilmente acessíveis a qualquer pessoa com acesso ao código ou conhecimento de engenharia reversa.

O mau gerenciamento de credenciais pode levar a vários impactos técnicos significativos. Usuários não autorizados podem obter acesso a informações ou funcionalidades confidenciais no aplicativo móvel ou em seus sistemas de back-end, isso pode levar a violações de dados, perda de privacidade do usuário, atividades fraudulentas e potencial acesso a funcionalidades administrativas das aplicações.

2.3.1.2 Segurança inadequada da cadeia de suprimentos

A segurança inadequada da cadeia de suprimentos é uma vulnerabilidade que permite a um atacante comprometer um componente de terceiros para injetar código malicioso. Por exemplo, se um invasor comprometer um repositório de código utilizado no desenvolvimento de um aplicativo ou modificar o código durante o processo de construção, poderá inserir um backdoor, spyware ou outro código malicioso, afetando a integridade do aplicativo final.

Isso pode permitir que o invasor roube dados, espione usuários ou assuma o controle do dispositivo móvel. Além disso, um invasor pode explorar vulnerabilidades em bibliotecas de software de terceiros, kits de desenvolvimento de software, fornecedores ou credenciais codificadas para obter acesso aos aplicativo móvel ou aos servidores back-end, isso pode levar ao acesso ou manipulação não autorizada de dados, negação de serviço ou controle total do aplicativo ou dispositivo móvel.

2.3.1.3 Autenticação/autorização insegura

Esse vulnerabilidade ocorre quando os aplicativos móveis não autenticam ou autorizam os usuários adequadamente. Isso pode causar uma falha em verificar as permissões adequadas, permitindo que um usuário não autorizado acesse dados ou funcionalidades restritas.

Um invasor pode explorar essas fraquezas de duas maneiras. Ele pode falsificar ou ignorar a autenticação enviando solicitações de serviço diretamente ao servidor do aplicativo móvel, contornando qualquer interação direta com o aplicativo móvel, ou podem fazer login no aplicativo como um usuário legítimo após passar com sucesso pelo controle de autenticação e então ir até um endpoint vulnerável para executar funcionalidades administrativas. Os métodos de exploração são normalmente realizados por meio de malware móvel no dispositivo, botnets de propriedade do invasor ou ferramentas de envio e interceptação de requisições.

2.3.1.4 Validação de entrada/saída insuficiente

A validação e sanitização de entrada/saída de dados insuficiente pode permitir a manipulação de dados de entrada do usuário a fim de forçar um comportamento indevido na aplicação, causando graves vulnerabilidades de segurança. Se um aplicativo não valida adequadamente esses dados, pode ser vulnerável a ataques de injeção de dados, como injeção de SQL, comandos ou javascript, onde um invasor manipula os dados de entrada para explorar falhas no sistema, arquitetura ou armazenamento da aplicação. Essas vulnerabilidades podem ter consequências prejudiciais, incluindo acesso não autorizado a

dados confidenciais, manipulação de funcionalidades de aplicativos e comprometimento potencial de todo o sistema móvel.

2.3.1.5 Comunicação Insegura

A comunicação insegura ocorre quando dados sensíveis são transmitidos sem proteção adequada. Se um aplicativo móvel, por exemplo, enviar informações de login sem usar uma conexão segura (HTTPS), os dados podem ser interceptados por um atacante durante a transmissão.

A maioria dos aplicativos móveis modernos troca dados com um ou mais servidores remotos. Quando a transmissão de dados ocorre, normalmente ela passa pela rede da operadora do dispositivo móvel e pela Internet. Um atacante que tem acesso a rede pode interceptar e modificar os dados se forem transmitidos sem nenhum método de segurança eficiente, podendo resultar no roubo de informações confidenciais, realização de espionagem, roubo de identidade e muito mais.

2.3.1.6 Controles de privacidade inadequados

Controles de privacidade inadequados referem-se à falta de medidas para proteger informações confidenciais dos usuários. Um exemplo seria um aplicativo que coleta dados pessoais sem consentimento explícito do usuário ou sem a implementação de práticas de segurança adequadas. Essas informações são valiosas para os invasores por N motivos, como por exemplo para personificar a vítima para cometer uma fraude, utilizar indevidamente os dados de pagamento da vítima, chantagear a vítima com informações confidenciais ou prejudicar a vítima destruindo ou manipulando seus dados críticos.

As fontes típicas de informações de identificação pessoal são geralmente bem protegidas, por exemplo, a sandbox do aplicativo, a comunicação de rede com o servidor, os logs e backups do aplicativo, etc. Alguns têm menos proteção, mas ainda são difíceis de acessar, como parâmetros de consulta de URL e conteúdo da área de transferência. Dessa forma, a obtenção dessa informação esta comumente ligada a violação da segurança em outro nível. Os invasores podem espionar a comunicação da rede, acessar o sistema de arquivos, a área de transferência ou os registros com um trojan ou colocar as mãos no dispositivo móvel e criar um backup para análise.

2.3.1.7 Proteções binárias insuficientes

Proteções binárias insuficientes podem ser exemplificadas por um aplicativo que não utiliza técnicas de ofuscação de código, permitindo que um atacante analise e com-

preenda facilmente o funcionamento interno do aplicativo por meio de engenharia reversa do mesmo, facilitando a exploração de vulnerabilidades.

O binário pode conter segredos valiosos, como chaves comerciais ou segredos criptográficos codificados que um invasor pode usar indevidamente - além de ser valioso por si só, por conter a lógica geral da aplicação, que facilita a compreensão e por consequência a exploração da aplicação.

Os invasores podem manipular binários de aplicativos para acessar recursos pagos gratuitamente ou para contornar outras verificações de segurança, além de coletar informações. Na pior das hipóteses, aplicativos populares podem ser modificados para conter códigos maliciosos e distribuídos por meio de lojas de aplicativos de terceiros ou sob um novo nome para explorar usuários desavisados.

2.3.1.8 Configuração incorreta de segurança

A configuração incorreta de segurança pode ocorrer quando as configurações do sistema ou do aplicativo não são devidamente ajustadas para mitigar riscos. Essas vulnerabilidades podem ir do uso de configurações padrão inseguras, que podem conter níveis de segurança fracas ou permissões desnecessárias habilitadas, até controles de acesso inadequados e métodos criptográficos atualmente considerados fracos.

Essas falhas são comuns em aplicativos móveis devido a fatores como restrições de tempo, falta de conhecimento ou erro humano durante o desenvolvimento; Detectalás é relativamente fácil por meio de revisão manual de código, testes de segurança ou ferramentas de verificação automatizadas.

2.3.1.9 Armazenamento de dados inseguro

O armazenamento de dados inseguro refere-se à prática de não proteger adequadamente os dados armazenados, o que pode atrair vários agentes de ameaças que visam explorar as vulnerabilidades e obter acesso não autorizado a informações confidenciais.

Tais agentes incluem adversários qualificados que atacam aplicativos móveis para extrair dados valiosos, pessoas mal-intencionadas dentro da organização ou da equipe de desenvolvimento de aplicativos que fazem uso indevido de seus privilégios, atores patrocinados pelo Estado que realizam espionagem cibernética, cibercriminosos que buscam ganhos financeiros por meio de roubo ou resgate de dados, entre outros.

Os vetores de ataque incluem acesso não autorizado ao sistema de arquivos do dispositivo por meios físicos ou remotos, exploração de criptografia fraca ou falta dela, interceptação de transmissões de dados e aproveitamento de malware ou aplicativos maliciosos instalados no dispositivo. Além disso, dispositivos com acesso root ou desbloqueados

oferecem uma oportunidade para os invasores contornarem as medidas de segurança e obterem acesso direto a dados confidenciais.

2.3.1.10 Criptografia insuficiente

A criptografia insuficiente é evidenciada quando a criptografia utilizada não oferece proteção adequada contra ataques podendo quebrar a confidencialidade, a integridade e a autenticidade de informações confidenciais. Por exemplo, se um aplicativo usar algoritmos de criptografia fracos ou chaves de tamanho insuficiente, os dados criptografados podem ser comprometidos mais facilmente por técnicas de quebra de criptografia.

Os atacantes podem empregar várias técnicas de criptoanálise, como ataques criptográficos, ataques de força bruta ou ataques de canal lateral, para explorar fraquezas em algoritmos de criptografia, gerenciamento de chaves ou falhas de implementação. Ao visar a criptografia insegura, os invasores pretendem descriptografar dados criptografados, manipular processos criptográficos ou obter acesso não autorizado a informações confidenciais. Isso pode levar a violações de dados, acesso não autorizado a contas de usuários, comprometimento da confidencialidade ou capacidade de falsificar ou adulterar dados.

Capítulo 3:
Revisão de literatura

Os serviços bancários móveis compartilham a necessidade crítica de segurança da informação, mas diferem em alguns aspectos de implementação e preocupações específicas de outros aplicativos (S.; SALEH, 2015).

3.1 Desafios e ameaças

Todos os tipos de sistemas são alvos de criminosos cibernéticos. Por conta disso, muitos mecanismos de segurança são adotados para garantir a segurança em aplicações financeiras.

Chen et al. (2020) realizam um estudo empírico abrangente e em grande escala sobre os 2.157 vulnerabilidades de segurança coletados de 693 aplicativos bancários em mais de 80 países, sob vários aspectos. Para coletar o conjunto de dados, também foi proposto um sistema de três fases, o AUSERA, para identificar automaticamente as vulnerabilidades relacionados a dados em aplicativos bancários. E por fim foram descritas essas vulnerabilidades, sendo grande parte delas relacionadas a problemas na implementação da criptografia, como utilização de métodos impróprios e inseguros; problemas na realização da autenticação, como autenticação inválida e falsificação; e problemas de armazenamento inseguro em arquivos de texto, SD Card, entre outros. Com isso, o estudo reduz as lacunas entre a investigação académica e os bancos industriais e ajuda tanto os bancos como as empresas terceiras a enfrentar melhor as deficiências de segurança.

Yildirim e Varol (2019) descrevem o banco móvel como mais fraco em termos de segurança do que o banco on-line tradicional, por fazer uso de conexões conexão sem fio em sistemas operacionais diversos, como IOS, Android e BlackBerry, o que torna mais difícil e complicado tomar medidas de segurança para todos os serviços bancários móveis. Assim ele examina que tipo de ameaças existem nos dispositivos móveis e as divide ameaças em três grupos: dispositivo, rede e data center. As falhas de dispositivo são relacionadas à aplicação, com problemas de permissão, manipulação e validação; ao sistema, com

questões relacionadas ao root e jailbreak no android, armazenamento de dados estáticos e senhas fracas. As falhas de rede referentes a ataques de Man-In-The-Middle e Sniffing, que são formas de interceptação, análise e até alteração de dados em transito; implementação ruim de criptografia na comunicação, como uso de métodos inseguros como ssl e wifi com criptografias fracas. E as falhas de data center dizendo sobre falhas muito citadas em aplicações WEB, como falhas de injeção de código malicioso, problemas de configuração, questões de validação, entre outras. Com base nas ameaças, ele divide propões como solução o uso de criptografia e certificados digitais da forma correta; Requisito de login, isso é, além do ID de usuário e senha de login, o uso de CAPTCHA e da autenticação de dois fatores, o que pode fornecer medidas de segurança adicionais para o usuário fazer login com segurança; Gerenciamento de sessões, que é proteger e gerenciar da maneira devida as informações de sessão do usuário; Tipo de entrada do usuário de login que é utilizar um teclado virtual para o usuário efetuar login com uma senha e alterar a posição de suas letras e números a cada processo de login, o que pode reduzir o risco potencial de ataques de malwares.

Darem et al. (2023) fornecem uma análise abrangente das ameaças cibernéticas nos setores bancário e financeiro, incluindo a identificação de ameaças comuns, a sua natureza e caráter e as classifica com base na sua gravidade e tecnicidade. Além disso, o artigo explora as contramedidas técnicas, não técnicas, organizacionais e as medidas legais e regulamentares utilizadas para proteger as transações financeiras contra ameaças cibernéticas. Dentre as ameaças técnicas, ele descreve Phishing e malware como ameaças graves, pois podem levar ao acesso não autorizado a informações confidenciais e transações financeiras. Ataques distribuídos de negação de serviço (DDoS), ataques à cadeia de suprimentos, ataques a aplicativos da web, ameaças bancárias móveis e ameaças à segurança na nuvem são outras ameaças técnicas que podem impactar os serviços bancários e financeiros. Ameaças a internet das coisas (IoT), ameaças de controle de conta, cryptojacking, explorações de zero days, ataques man-in-the-middle, ataques de senha, preenchimento de credenciais, deepfakes e desinformação, vulnerabilidades de dia zero, ameaças de computação quântica e os riscos dos fornecedores também são ameaças potenciais aos serviços bancários e financeiros. Com tudo isso, o artigo propõe contramedidas destinadas a mitigar o impacto e reduzir as vulnerabilidades associadas a essas ameaças cibernéticas. O uso de Criptografia em dados em repouso e em transito, segmentação de rede para reduzir o movimento lateral de usuários, Firewalls e IPS para a proteção da infraestrutura e autenticação por dois fatores, foram alguns métodos de segurança listados pelo autor. Além de apenas contramedidas técnicas, o autor também define questões legais e organizacionais como prioridade na implementação segura de aplicações bancárias.

Ubaldo et al. (2023) realizam uma análise bibliográfica, que permitiu conhecer as lacunas do conhecimento a cerca da segurança da informação no setor bancário. Os artigos analisados listam os ataques cibernéticos mais recorrentes que ameaçam a segu-

rança da informação no setor bancário ataques, dentre eles estão ataques por Malwares, Phishing, violações de dados, DoS e XSS. O autor diz que a falta de um gerador eléctrico de reserva, falhas na proteção de firewall, falta de auditorias de segurança da informação, falta de gerenciamento de controle de criptografia e falta de proteção da verdadeira identidade dos usuários são os cinco fatores mais críticos a se considerar. Além disse, ele enfatiza que os sistemas de segurança bancária devem ser concebidos com muito cuidado, considerando muitos fatores diferentes no processo, não apenas internos à infra-estrutura bancária, mas também sistemas externos. Com isso, ele conclui que biometria, campanhas de conscientização ao phishing, introdução de tokens de software e hardware, atualização constante sobre os avanços tecnológicos e a continuação do investimento na cibersegurança são pontos extremamente importantes na concepção de aplicações bancárias.

Chandra sekhar e Kumar (2023) analisam os ataques cibernéticos no setor bancário e a forma de fornecer segurança cibernética a esses ataques. Dentra as orincipais ameaças estão Dados não criptografados, que ocorre quando os dados são deixados sem criptografia (não ocultos) e esses dados foram facilmente usados por hackers ou cibercriminosos; Malware, que realizam ataques sérios aos bancos digitais, hackeando os dados confidenciais que passam pela rede, manipulando a aplicação, entre outros riscos; serviços de terceiros, que trazem um risco a mais ao negório e a necessidade da confiabilidade ao serviço solicitado; Falsificação, quando os cibercriminosos conseguem simular a URL do site do banco que se parece com o site original; e o Phishing que é a ameaça cibernética mais antiga e popular no setor bancário, onde um atacante tenta obter informações confidenciais da vítima por meio de e-mail/chamada, telefônica ou SMS. Dessa forma, o artigo comunica a necessidade da utilização da criptografia nos dados a fim de torna-los ocultos em formato ilegível, uso de aplicativos antimalware para combater os ataques diretamente do próprio dispositivo, a conscientização do consumidor para informar a todos os usuários medidas e comportamentos padrões da instituição, entre outros métodos de segurança.

Falade e Ogundele (2023) analisam as vulnerabilidades de aplicações dos bancos digitais do Reino Unido para identificar vulnerabilidades nas aplicações e oferecer contramedidas que possam ajudar a melhorar a segurança das aplicações bancárias. Alguns dos riscos gerais citados no artigo e encontrados em aplicações bancárias móveis e na utilização de dispositivos móveis em geral são: códigos e aplicações maliciosos, violação de privacidade, infraestrutura de pagamento, infraestrutura de operadora sem fios e vulnerabilidades de SMS. Outras ameaças incluem: espionagem, malware, falta de conhecimento do usuário, ameaça de aplicativos de terceiros, phishing, mau funcionamento da plataforma, negação de serviço, Wi-Fi não criptografado, mau funcionamento de aplicativos/dispositivos, acesso não autorizado e perda, roubo ou descarte inadequado do dispositivo. No topo da lista de problemas de segurança dos aplicativos bancários móveis está a fraude e o roubo de identidade. Os autores também realizam uma análise de vulnerabilidade estática em seis aplicações bancárias utilizando um scanner de vulnerabilidade automatizado de

código aberto, o AndroBugs, e em todas as aplicações foram encontradas e descritas as vulnerabilidades. Com tudo, o artigo propõe uma lista de extensa de contramedidas para cada uma das ameaças citadas, além de medidas comportamentais para o usuário, a fim da implementação segurança e consciente das aplicações bancárias.

Alzoubi et al. (2022) analisam o problema de segurança que geralmente ocorre quando se trata de serviços bancários digitais por meio de trabalhos de pesquisa anteriores realizados por outros autores sobre o tema. Os principais problemas citados no artigo são dados não criptografados, Malware, serviços de terceiros não confiáveis, utilização de dados manipulados e Spoofing. Conhecendo as diferentes maneiras pelas quais os criminosos cibernéticos costumam tirar vantagem do banco digital plataformas, o artigo propõe como solução a utilização de um sistema de autenticação multi-emissões com os seguintes tópicos: Emissão de certificados digitais, tokens OTP, proteção do navegador, monitoramento transacional e criptografia dos dados.

Wodo, Stygar e Błaśkiewicz (2021) analisam os perigos e métodos associados ao uso de tecnologias bancárias digitais e móveis por pessoas com diferentes níveis de conscientização sobre ameaças relacionadas à TI e descrevem a segurança de aplicações bancárias. A primeira linha de proteção é o próprio dispositivo em que utilizamos serviços bancários portanto devemos garantir que apenas uma pessoa autorizada possa utilizá-los. No caso de um dispositivo móvel, proteção de acesso baseada em uma senha ou PIN longo (pelo menos 6 a 8 caracteres) pode ser o cumprimento mínimo deste critério. A solução baseada em biometria pode melhorar adicionalmente a ergonomia da solução e impossibilita a quebra da senha, pois os recursos biométricos são mais difíceis de obter pelo adversário. Do ponto de vista do aplicativo bancário, uma boa ideia é verificar se o dispositivo não está desprovido de segurança padrão (Root ou Jailbreak). A segurança da rede através da qual usamos serviços bancários é também um elemento fundamental e deve ser assegurado que as operações financeiras sensíveis sejam realizadas em redes confiáveis ou pelo menos bem protegidas. A TFA por cartões SIM é um problema essencial associado aos serviços bancários eletrônicos e móveis porque a grande maioria dos bancos e outras instituições financeiras promovem este mecanismo de segurança como um meio seguro forma de confirmar transações. Outros possíveis métodos de TFA são TOTP (hardware ou software), assinatura eletrônica, etc.

Stanikzai e Shah (2021) avaliam a eficácia dos métodos de segurança cibernética existentes na redução ou mitigação do crime financeiro e criam recomendações de segurança para melhorias potenciais. O artigo classifica os ataques a aplicações bancárias em dois tipos: aqueles que visam e danificam diretamente redes ou dispositivos informáticos, como malware, ataques de injeção de código macilioso e ataques de negação de serviço; e aqueles que são facilitados por redes ou dispositivos informáticos, mas têm um propósito que não esteja relacionado à rede ou dispositivo de computador, como fraude, roubo

de identidade, golpes de phishing, guerra de informação ou cyberbullying. Como solução os autores propõe algumas das tecnologias e comportamentos modernos utilizadas na segurança cibernética: Scanner de vulnerabilidade, para automatizar a busca de vulnerabilidades nos aplicativos; sistemas de prevenção e detecção de intrusões, para identificar e prevenir o acesso ilegal aos recursos ou infraestrutura da empresa; e um quadro cíclico de segurança cibernética, isso é, um programa ou política de segurança cibernética documentada para realizar a gestão de risco de governação, identificação, proteção, identificação, reação e recuperação de maneira periódica. Além disso, o artigo lista caso de ataque financeiro anual dos Bancos Centrais Mundiais, o que nos permite entender detalhes do comportamento de hacker pelo mundo durante ataques reais.

Boitan (2019) chama a atenção para os riscos de segurança cibernética a que o setor financeiro está exposto, que recentemente começaram a suscitar uma preocupação crescente entre as autoridades europeias e internacionais, em termos de prevenção, identificação, avaliação e gestão adequadas. As violações de dados registradas como incidentes cibernéticos podem ser representadas por: roubo de dados de clientes ou de dinheiro de contas de clientes, acesso não autorizado a informações e bancos de dados de clientes usando login interno, phishing, interrupção de negócios. Por fim, o autor afirmam que mais análises precisam de ser realizadas de modo a visar as ameaças emergentes à estabilidade financeira e é necessário que o setor financeiro continue a investir na cibersegurança.

Bilal e Sankar (2023) descreve o risco do uso de dispositivos móveis para pagamentos, bem como as precauções e medidas de segurança que podem ser implementadas para tornar essas aplicações seguras. Os autores enfatizam que existem uma variedade de cenários de risco de segurança cibernética dos quais indivíduos e organizações devem estar cientes, como ataques de phishing, malwares, ataques de engenharia social e ameaças internas. E ressalta que estes cenários de risco de segurança cibernética mostram como é crucial tomar medidas proativas para se proteger contra perigos potenciais por meio da implementação de defesas de segurança robustas, como mecanismos de autenticação seguros, Criptografia moderna, canais de comunicação seguros e detecção de fraudes em tempo real. Com isso o artigo conclui que ao priorizar a segurança e a transparência, os provedores de serviços bancários móveis podem construir essa confiança e continuar a aumentar a sua base de usuários.

Liu, Wang e Peng (2020) descrevem como métodos essenciais do pagamento em dispositivos móveis a tokenização, que é o processo de substituição de informações sensíveis por um token; a segurança na ligação e utilização do número do cartão, concluindo que ela deve ser feita por meio de protocolos baseados em confiança e anti-vazamento; e a autenticação, que é um processo de segurança feito para verificar a veracidade e autenticidade de uma pessoa, objeto ou ação. Utilizando esses métodos da maneira devida, o artigo conclui que boa parte das necessidades do pagamento móvel são supridas.

Wang, Hahn e Sutrave (2016) descrevem muitos métodos que pode ser utilizados em aplicações bancárias. Sendo o uso de impressão digital e autenticação multifatorial como método de autenticação de ações, transações e usuários, TLS e uso de certificados para uma comunicação segura, entre outros. Ele também descreve muitos desafios, ameaças e ataques. Malwares, vulnerabilidades de redes e certificados, vazamento de informações, remediação de ameaças de pagamento móvel, são algumas ameaças consideráveis durante a implementação de segurança. Com base nisso, são citados os principais desafios de segurança que deve-se entender e superar, como a detecção de malware, autenticação de maneira geral, prevenção de violação de dados e detecção e proteção contra fraudes. Contudo, para remediar os riscos dos pagamentos móveis, tanto os utilizadores como os prestadores de serviços de pagamentos móveis precisam de tomar medidas para proteger a segurança e evitar violações de dados.

Hassan, Shukur e Mohd (2022) realizam uma série de testes de segurança com o objetivo de avaliar os principais aplicativos de finanças utilizados na Malásia. Foi feita somente a análise do código fonte da aplicação por meio de ferramentas automatizadas, o que diminui o tempo de teste e facilita a análise contínua das presentes aplicações. A análise deduz que todos os aplicativos seguem algum tipo de padrão de segurança, mas seus recursos e propriedades de segurança são diferentes. Com isso, foram identificadas as aplicações bancárias móvel mais e menos seguras com base nas suas métricas de segurança utilizadas pelas ferramentas escolhidas. Entender essas abordagens nos permite ter certa noção de como um atacante real atuaria e ameaças encontradas nessa área.

Datta et al. (2020) disseta principalmente sobre o número crescente de casos de fraude online relacionados com o setor bancário chegando a conclusão que programas de conscientização são necessários entre os clientes bancários para prevenir ou evitar diversos tipos de fraudes online.

Capítulo 4:
Metodologia da Pesquisa

Este trabalho parte de uma artigo de revisão. Conforme citado por Martins e Pinto (2001), a revisão de bibliográfica é o momento em que o autor faz uso de diferentes trabalhos publicados em livros, revistas, periódicos e outros, para que sirva de base para suas análises. Este tipo de pesquisa tem como finalidade colocar o pesquisador em contato direto com tudo o que foi escrito, dito ou filmado sobre determinado assunto a fim de obter conclusões. Um artigo de revisão não é apenas uma mera repetição do que já foi dito ou escrito sobre determinado assunto, mas sim, proporciona o exame de um tema sob novo enfoque ou abordagem, chegando a conclusões inovadoras (LAKATOS; MARCONI, 2021).

4.1 Levantamento de dados

Para a confecção do presente trabalho foram utilizados artigos científicos encontrados em plataformas públicas como Google Scholar, Sci-hub e Typeset.io por meio das palavras chave Mobile Banking Security e com a data da publicação entre os anos de 2019 e 2024. Como questões da pesquisa foram escolhidas as seguintes perguntas:

- Quais são as ameaças de segurança mais críticas do setor bancário no android?
- Quais são os métodos de segurança mais eficazes e viáveis para combater essas ameaças?

Com isso, foram selecionados artigos científicos com conteúdo técnico voltado ao pesquisador e desenvolvedor de aplicações bancárias com foco em segurança da informação, publicados em língua inglesa e com texto completo disponível. Dessa forma, evitando artigos não relacionados ao tema, incompletos, não publicados em língua inglesa e com conteúdo não técnico, isso é, artigos para usuários.

E por fim, optou-se por selecionar quais ajudariam a responder as questão de pesquisa com base em seu título, palavras-chave e resumo.

4.2 Análise de dados

Após a coleta dos dados, procedeu-se à leitura detalhada do material, chegando na compilação das informações mais relevantes. Em seguida, foi conduzida uma análise descritiva, que visou não apenas compreender, mas também aprofundar o conhecimento sobre o tema investigado. Essa análise descritiva permitiu identificar padrões e tendências nos dados, contribuindo para a construção de um referencial teórico robusto e fundamentado, essencial para a compreensão aprofundada da segurança em aplicações bancárias móveis e por fim a idealização do modelo proposto seguidamente.

Capítulo 5:
Resultados

O objetivo principal desse trabalho é entender os pontos críticos e os principais métodos de segurança da informação em aplicações de bancárias no sistema Android a partir da leitura e análise de bibliografias passadas.

5.1 Componentes chave

Entender os componentes chave de segurança em aplicações bancárias no Android é essencial para garantir a proteção dos dados dos usuários e a integridade das transações financeiras. Em primeiro lugar, fica claro como uma das maiores ameaças a serem enfrentadas são os malwares. Esses softwares maliciosos podem se infiltrar nos dispositivos dos usuários através de aplicativos falsos ou comprometidos, visando roubar informações sensíveis, como credenciais bancárias e dados pessoais. Podemos concluir também que ataques de autenticação representam um risco sério, onde cibercriminosos tentam comprometer o processo de login de usuários para obter acesso não autorizado às suas contas. Outra grande preocupação é a criptografia, que se implementada de maneira inadequadamente podem ser facilitar a interceptação e decifração dos dados por atacantes, expondo informações sensíveis. Por fim, ataques de rede representam uma ameaça constante para as aplicações bancárias móveis. Esses ataques ocorrem quando um atacante intercepta e possivelmente altera a comunicação entre o usuário e o servidor bancário.

5.2 Arquitetura de aplicações bancárias

A arquitetura do sistema desempenha um papel crucial na construção de plataformas financeiras digitais seguras, eficientes, confiáveis e centrados no usuário. Dessa forma, ela devem ser projetadas para garantir a segurança, escalabilidade e adaptabilidade às mudanças tecnológicas. No contexto de um banco móvel, a arquitetura geralmente com-

preende camadas distintas, incluindo o front-end, responsável pela interface do usuário intuitiva e acessível, o back-end que gerencia a lógica de negócios e a manipulação segura de dados, e a camada de segurança, incorporando autenticação robusta e criptografia para proteger a confidencialidade das informações financeiras dos usuários.

Como proposto por S. e Saleh (2015), as aplicações bancárias móvel carregam uma arquitetura simples por conter apenas ações e validações internas da própria instituição, como pode-se ver na figura 6. O dispositivo utilizado, que é acessado pelo usuário para interagir com o sistema, exibi os menus e transmite mensagens curtas de forma segura. A plataforma do banco facilita a transferência de mensagens curtas para comandos bancários compatíveis. A interação entre o usuário e o provedor de serviços ocorre por meio de diálogos multiníveis, com o banco fornecendo suporte e executando instruções nas contas bancárias. O Sistema de banco móvel também suporta a comunicação com outros servidores contribuindo para a ampliação dos serviços oferecidos ao usuário.

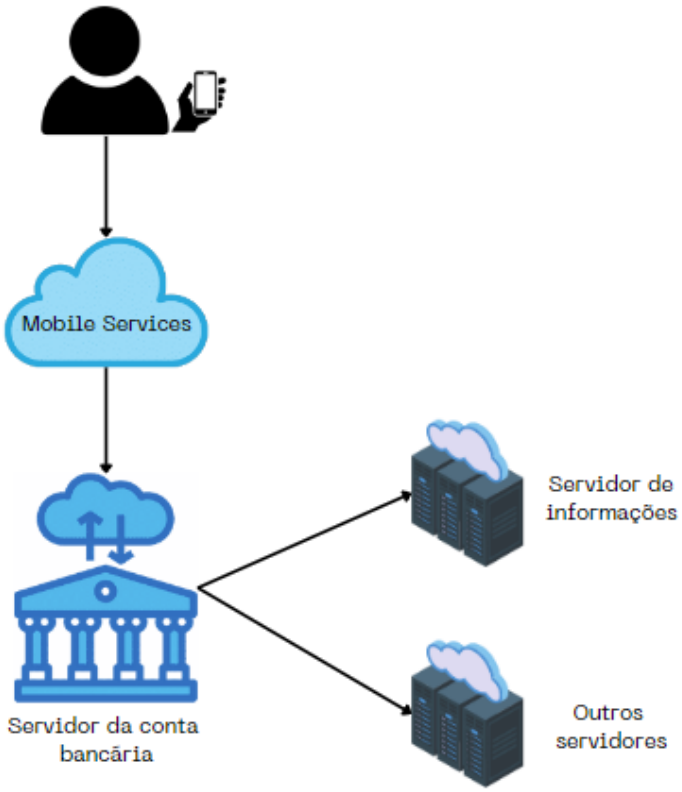

Figura 6 – Arquitetura de uma aplicação de banco móvel

5.3 Métodos de segurança

Em sua essência, este modelo conceitual destaca a necessidade de um conjunto unificado de diretrizes que não apenas mitigue riscos amplos, como acesso não autorizado

e alteração de dados, mas também abranja diversas dimensões de segurança, incluindo criptografia, autenticação, entre outros fatores.

Os métodos de segurança utilizados para esse fim são compostos por 4 áreas de segurança entendidas mais as críticas da superfície de ataque de aplicativos bancários móvel: Comunicação entre processos, criptografia, autenticação e segurança de redes. Áreas essas que se ramificam como podemos ver na figura 7, e cada uma delas está descrita e exemplificada abaixo utilizando como base a LLC (2024).

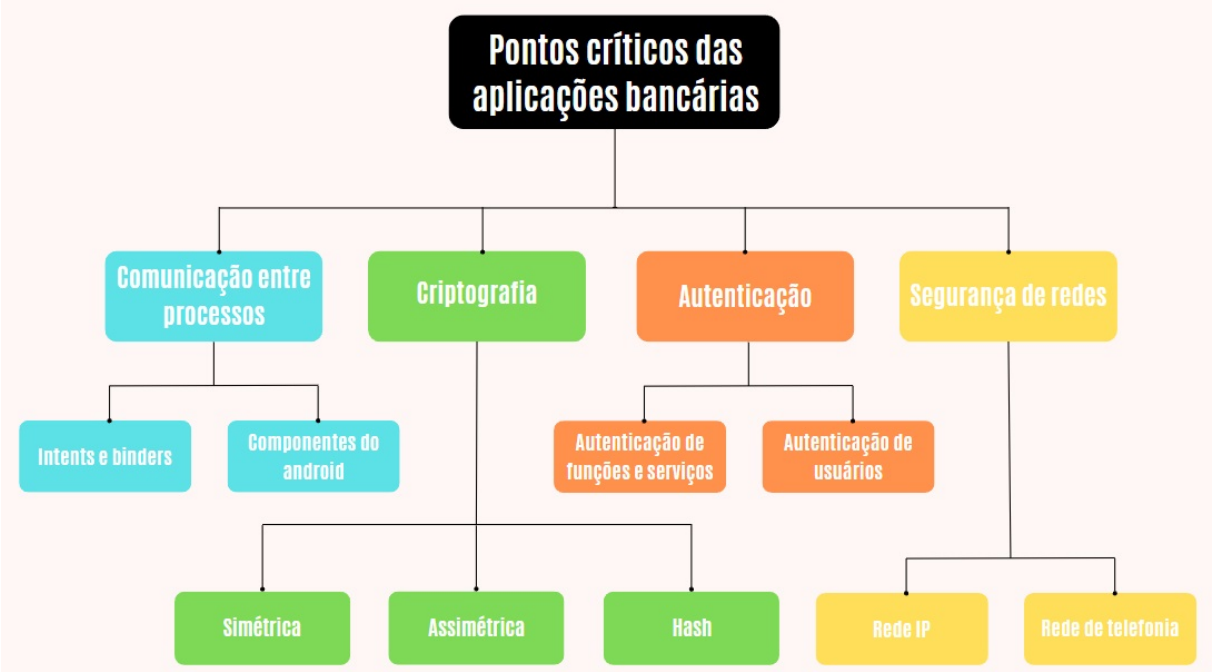

Figura 7 – Árvore de métodos de segurança

5.3.1 Comunicação entre processos

A comunicação entre processos (IPC, Inter-Process Communication) no Android é um aspecto crucial do desenvolvimento de aplicações, permitindo que componentes de diferentes aplicações ou de diferentes partes de uma mesma aplicação possam interagir de maneira segura e eficiente. O Android oferece várias ferramentas e mecanismos para facilitar essa comunicação, incluindo Intents e Broadcast Receivers, cada um com suas funcionalidades específicas e usos recomendados.

5.3.1.1 Intents e Binders

Intents são a principal forma de comunicação entre componentes no Android e podem ser usados para iniciar atividades, serviços e transmitir mensagens entre diferentes

partes de uma aplicação ou entre aplicações diferentes. Existem dois tipos principais de intents: explícitos e implícitos. Intents explícitos são utilizados para iniciar um componente específico dentro da mesma aplicação, identificando-o diretamente pelo nome da classe. Intents implícitos, por outro lado, não especificam o componente diretamente; em vez disso, declaram uma ação geral a ser realizada, permitindo que o sistema determine a aplicação ou componente adequado para lidar com a solicitação. Este mecanismo facilita a integração entre diferentes aplicações e permite uma comunicação mais flexível. Contudo, seu uso inadequado pode levar a graves problemas de segurança. um invasor pode controlar parcial ou totalmente o conteúdo de uma intenção usada para iniciar um novo componente no contexto de um aplicativo vulnerável. Antes de processar um Intent recebido, é crucial validá-lo para garantir que ele está sendo redirecionada para um pacote seguro, por meio do método 'ResolveActivity()', e limpar adequadamente as informações agrupadas com o 'IntentSanitizer'.

```
1    // Verificação
2    Intent intent = getIntent()
3    Intent forward = (Intent) intent.getParcelableExtra("key");
4    ComponentName name = forward.resolveActivity(
        getPackageManager());
5    if (name.getPackageName().equals("safe_package") &&
6            name.getClassName().equals("safe_class")) {
7         startActivity(forward);
8    }
9
10   // Sanitização
11   Intent intent = new  IntentSanitizer.Builder()
12    .allowComponent("com.example.ActivityA")
13    .allowData("com.example")
14    .allowType("text/plain")
15    .build()
16    .sanitizeByThrowing(intent);
```

Listing 5.1 – Verificação e sanitização de Intent

Outra importante mecânica de IPC no Android é a Binder, que fornece um mecanismo de chamada de procedimento remoto (RPC), sendo considerado a espinha dorsal da IPC no Android e permite que diferentes processos compartilhem dados de forma segura e eficiente. Ele funciona criando uma interface através da qual os processos podem se comunicar como se estivessem fazendo chamadas de método locais, assim, sendo útil para serviços que precisam fornecer funcionalidades para outras aplicações de forma segura. A segurança no uso do Binder é garantida através do controle de permissões e da verifica-

ção de identidades, assegurando que apenas processos autorizados possam se comunicar e utilizar recursos entre si.

```
1    // Controle de Permissões
2    @Override
3    public boolean onTransact(int code, Parcel data, Parcel reply
        , int flags) throws RemoteException {
4        if (checkCallingPermission("com.example.PERMISSION") ==
            PackageManager.PERMISSION_DENIED) {
5            return false;
6        }
7
8        return super.onTransact(code, data, reply, flags);
9    }
10
11   // Verificação de Identidade do Chamador
12   @Override
13   public void someMethod() {
14       int callingUid = Binder.getCallingUid();
15       String callingPackage = getPackageManager().getNameForUid
            (callingUid);
16       if (!"com.example.trustedapp".equals(callingPackage)) {
17           throw new SecurityException("Unauthorized access");
18       }
19   }
```

Listing 5.2 – Controle e verificação de identidade de Binder

5.3.1.2 Componentes do Android

O Android também oferece componentes como o Content Providers, que são componentes que gerenciam acesso a um conjunto estruturado de dados. Eles são frequentemente usados para compartilhar dados entre diferentes aplicações, como contatos ou arquivos multimídia, utilizando URIs (Uniform Resource Identifiers) e métodos CRUD (Create, Read, Update, Delete) para identificar e manipulação dados específicos. Esses componentes permitem restringir o acesso a esses dados através de permissões específicas, garantindo que apenas aplicações autorizadas possam acessar ou modificar as informações.

Outro componentes são as Broadcast Receivers, que permitem que uma aplicação responda a mensagens enviadas por outras aplicações ou pelo próprio sistema. Esse componente podem ser usados para várias finalidades, como responder a eventos do sistema (por exemplo, mudança de conectividade) ou comunicar eventos internos entre diferentes componentes de uma aplicação. Quando um evento é disparado, o sistema envia um Intent

para todos os Broadcast Receivers registrados para aquele evento, permitindo que cada receiver execute uma ação em resposta ao evento.

Componentes sensíveis, como providers e receivers, não devem ser acessíveis a outras aplicações sem nenhum tipo de proteção adequada. A exportação de componentes permite que outros aplicativos acessem e interajam com eles, o que pode representar um risco de segurança se não for devidamente controlado. É recomendável definir a propriedade "android:exported"de componentes sensíveis no manifesto da aplicação. Componentes que não precisam ser acessíveis por outros aplicativos devem ter essa propriedade definida como false. Isso restringe o acesso apenas ao próprio aplicativo, garantindo que os dados sensíveis não sejam expostos inadvertidamente.

```
1    <activity android:name=".SensiveActivity" android:exported="
        false" >
2        <intent-filter>
3            <action android:name="EXAMPLE_ACTIVITY" />
4            <category android:name="android.intent.category.
                LAUNCHER" />
5        </intent-filter>
6    </activity>
7
8    <service
9        android:name=".MessagingService"
10       android:exported="false">
11       <intent-filter>
12           <action android:name="com.google.firebase.
                MESSAGING_EVENT" />
13       </intent-filter>
14   </service>
15
16   <receiver android:name=".SensiveReceiver" android:exported="
        false">
17       <intent-filter>
18           <action android:name="EXAMPLE_BROADCAST" />
19       </intent-filter>
20   </receiver>
```

Listing 5.3 – Componentes exportados

Caso seja necessário a exportação, é fundamental definir permissões de segurança apropriadas para componentes sensíveis. Por exemplo, componentes podem exigir permissões específicas (READ_PROVIDER e WRITE_PROVIDER) ou assinaturas para

acessar e modificar dados. Assim, garantindo que apenas aplicativos autorizados com as devidas permissões ou assinados digitalmente da maneira esperada possam acessar componentes sensíveis, ajudando a mitigar possíveis vulnerabilidades.

```
1    <permission android:name="com.example.myapp.MY_PERMISSION"
        android:protectionLevel="signature" />
2
3    <provider
4        android:name=".MyContentProvider"
5        android:authorities="com.example.myapp.provider"
6        android:exported="true"
7        android:permission="android.permission.READ_PROVIDER">
8    </provider>
```

Listing 5.4 – Permissões no Android Manifest

5.3.2 Criptografia

A criptografia é a área que estuda e pratica princípios e técnicas para comunicação segura na presença de terceiros. A ideia principal é tornar impossível a leitura de uma mensagem por pessoas não autorizadas através da conversão de dados de um formato legível para um formato codificado. Ela é dividida em principalmente 3 tipos: Simétrica ou de chave privada, assimétrica ou de chave pública e Hash. Cada um desses 3 tipos de criptografia tem seus propósitos, forças e fraquezas.

5.3.2.1 Simétrica

São algoritmos criptográficos que usam a mesma chave para criptografar e descriptografar uma mensagem. A chave, na prática, representa um segredo compartilhado entre duas ou mais partes que pode ser usado para manter uma conexão de informação privada.

A segurança desse algoritmo está diretamente ligada a chave, como é transmitida e como é realizada a operação. Em alguns casos, se executada de maneira errada ou simples, esse algoritmo está aberto a criptoanálise, o que possibilita a quebra a cifra. Dessa forma, é possível destacar alguns algoritmos de criptografia simétrica, como o AES, DES e Blowfish.

A implementação de criptografia simétrica é fundamental para garantir a segurança dos dados em várias aplicações comerciais e pessoais. Para assegurar a máxima eficácia e

proteção, é essencial seguir diretrizes e recomendações específicas que abordem aspectos cruciais como a escolha e uso dos algoritmos, a gestão de chaves e a integridade dos dados.

Para fins comerciais, é altamente recomendável utilizar o AES com uma chave de 256 bits, que oferece um nível elevado de segurança adequado para a maioria das aplicações sensíveis. Caso o AES de 256 bits não esteja disponível, o uso do AES de 128 bits ainda proporciona uma segurança robusta e é preferível a algoritmos menos seguros.

Para garantir a integridade dos dados criptografados, é crucial escolher o modo de operação, que é a forma pelo qual o texto plano é submetido a criptografia, adequado do algoritmo AES. Dois modos de operação recomendados são o CBC (Cipher Block Chaining) e o CTR (Counter). Ambos os modos oferecem benefícios distintos em termos de segurança e desempenho. No modo CBC, cada bloco de texto cifrado depende do bloco anterior, garantindo que uma alteração em um bloco afete todos os blocos subsequentes. Este encadeamento fornece uma camada adicional de proteção contra certos tipos de ataques. No modo CTR, um contador é usado para gerar um fluxo de chave que é combinado com o texto claro para produzir o texto cifrado. O modo CTR oferece a vantagem de permitir criptografia e descriptografia paralelas, melhorando o desempenho em sistemas de alta demanda.

Um aspecto crítico na implementação de criptografia simétrica é a gestão adequada do vetor de inicialização (IV) ou contador. O IV deve ser criptograficamente aleatório e único para cada operação de criptografia para evitar vulnerabilidades que poderiam ser exploradas por atacantes. A reutilização do IV pode comprometer seriamente a segurança da criptografia, permitindo que um atacante identifique padrões e possivelmente recupere dados sensíveis. Para garantir a aleatoriedade, o IV deve ser gerado usando um gerador de números aleatórios seguro. Além disso, o IV deve ser transmitido junto com o texto cifrado para permitir a correta descriptografia pelo destinatário. No entanto, o IV em si não precisa ser mantido em segredo, pois sua segurança depende de sua unicidade e aleatoriedade.

Uso de criptografia simétrica para ocultação de dados:

```
1     byte[] plaintext = "Texto plano";
2     KeyGenerator keygen = KeyGenerator.getInstance("AES");
3     keygen.init(256);
4     SecretKey key = keygen.generateKey();
5     Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5PADDING");
6     cipher.init(Cipher.ENCRYPT_MODE, key);
7     byte[] ciphertext = cipher.doFinal(plaintext);
8     byte[] iv = cipher.getIV();
```

Listing 5.5 – Criptografia AES em java

5.3.2.2 Assimétrica

São sistemas criptográficos que utilizam pares de chaves para criptografar e descriptografar uma mensagem, gerar chaves, entre outras funções. Uma característica dessa criptografia é a dependência de conjunto de chaves para o seu uso e a sua segurança, sendo geralmente uma chave pública e acessível a todos e uma chave privada restrita ao indivíduo. Ao saber apenas a chave pública do par, não é possível ler a mensagem.

Esses algoritmos são baseados em cálculos matemáticos que são simples de se fazer mas custosos de se desfazer. O compartilhamento de uma chave pública para encriptação e utilização de uma chave privada para decriptação é um método de utilização muito forte para o envio seguro de mensagem, mas não tão rápido, então esse algoritmo é geralmente usado para troca e geração de chave e assinatura digital. Podem ser citados o protocolo de Diffie-Helmann, criptografia de curva elíptica e o RSA, como principais algoritmos assimétricos.

A criptografia assimétrica é uma técnica fundamental para garantir a segurança em diversas aplicações, proporcionando mecanismos seguros para a troca de chaves, autenticação e integridade de dados. Para assegurar a eficácia e a proteção dos dados, é essencial seguir diretrizes específicas e utilizar algoritmos modernos e bem estabelecidos. Algumas das melhores práticas para a implementação segura de criptografia assimétrica é o uso de criptografia de curva elíptica (ECC).

A criptografia de curva elíptica é amplamente reconhecida por sua eficiência e segurança. Comparada a outros algoritmos, a ECC oferece um nível elevado de segurança com chaves menores, o que resulta em melhor desempenho e menor consumo de recursos. Para garantir a segurança em sua implementação é recomendável utilizar chaves públicas de 224 ou 256 bits que proporcionam um equilíbrio ideal entre segurança e desempenho. A ECC com chaves de 256 bits, por exemplo, oferece um nível de segurança comparável ao RSA com chaves de 3072 bits, mas com uma carga computacional significativamente menor. Curvas Elípticas são boas para criptografia mas geralmente são utilizadas para a criação de assinaturas digitais com Elliptic Curve Digital Signature Algorithm (ECDSA) ou geração e troca de chaves com o Elliptic Curve Diffie-Hellman Ephemeral (ECDHE).

Uso de criptografia assimétrica para geração e verificação de assinaturas digitais:

```
1    // Gerando uma assinatura digital
2    byte[] message = "Texto plano";
3    PrivateKey key = "Chave Privada";
4    Signature s = Signature.getInstance("SHA256withECDSA");
5    s.initSign(key);
6    s.update(message);
```

```
7       byte[] signature = s.sign();
8
9
10      // Verificando uma assinatura digital
11      byte[] message = "Texto plano";
12      byte[] signature = "Assinatura";
13      PublicKey key = "Chave Pública";
14      Signature s = Signature.getInstance("SHA256withECDSA");
15      s.initVerify(key);
16      s.update(message);
17      boolean valid = s.verify(signature);
```

Listing 5.6 – Assinatura digital em Java com ECDSA

5.3.2.3 Hash

O hash criptográfica é uma algoritmo matemático que mapeia dados de qualquer tamanho para uma string de bits de tamanho fixo, considerado muito simples de fazer mas praticamente impossível de reverter, isto é, de recriar o valor de entrada utilizando somente o valor de dispersão. Esses algoritmos podem ser usados para assinatura, autenticação, entre outras funções que podem ser muito úteis de várias maneiras para a segurança da informação, entretanto podem ser problemáticas caso sejam vulneráveis. Alguns algoritmos muito utilizados são os algoritmos da família SHA, BCrypt e o PBKDF2.

A implementação de hash criptográfico é uma prática fundamental para garantir a integridade e autenticidade dos dados em várias aplicações de segurança. Funções de hash criptográfico geram uma representação fixa de dados de tamanho arbitrário, servindo como impressões digitais únicas. Para assegurar a segurança e a eficácia das funções de hash, é crucial seguir diretrizes e recomendações específicas.

Um dos principais requisitos para uma função de hash criptográfico segura é a resistência a colisões. Colisão ocorre quando duas entradas distintas produzem o mesmo valor de hash. Algoritmos de hash suscetíveis a colisões podem ser explorados por atacantes para subverter a integridade dos dados, levando a possíveis violações de segurança. Algoritmos mais antigos, como MD5 e SHA-1, são conhecidos por suas vulnerabilidades a colisões. Ataques práticos contra esses algoritmos foram demonstrados, tornando-os inadequados para aplicações de segurança modernas. Portanto, é essencial evitar o uso de tais algoritmos e adotar alternativas mais seguras.

SHA-256 (Secure Hash Algorithm 256-bit) é amplamente reconhecido como um dos algoritmos de hash mais seguros atualmente disponíveis. Parte da família SHA-2, o SHA-256 produz um hash de 256 bits, oferecendo uma forte resistência a geração de

colisões e a preimage attacks (ataques que tentam encontrar uma mensagem que produz um hash específico) e assegurando que os dados não possam ser facilmente manipulados ou falsificados.

Uso de Hash criptográfico para armazenamento de dados ou verificação de integridade:

```
1    byte[] message = "Texto plano";
2    MessageDigest md = MessageDigest.getInstance("SHA-256");
3    byte[] digest = md.digest(message);
```

Listing 5.7 – Uso de Hash em Java

5.3.3 Autenticação

Autenticação, como o nome já diz, é o processo de comprovar a veracidade das informações que temos, seja em um login de usuário ou na realização de um pagamento, que devemos ter certeza que a conta tentando realizar o pagamento ou o login é de fato da pessoa que está por trás do dispositivo móvel. Ela é um pré-requisito para muitas operações de segurança importantes e tem o objetivo de controlar o acesso a recursos protegidos, como dados do usuário, funcionalidade das aplicações e outros recursos.

5.3.3.1 Autenticação de funções e serviços

As funções e serviços de uma aplicação são as ações que um usuário pode realizar durante o seu uso; isso é, são todas as coisas que ele pode fazer, como por exemplo pagamento de boletos, transferências bancárias, entre outros. Essa autenticação pode ser feita de várias formas, sendo as mais comuns a senha numérica ou PIN e a biometria.

A autenticação por PIN é um método amplamente utilizado para proteger o acesso a aplicativos e dados no Android. Este método, baseado em uma senha numérica pré-criada, oferece uma camada adicional de segurança de forma simples e eficaz. No entanto, a implementação de autenticação por PIN deve ser realizada em um servidor e com muito cuidado para evitar vulnerabilidades. A segurança de um PIN depende significativamente de seu comprimento e complexidade. Embora PINs de 4 dígitos sejam comuns, recomenda-se o uso de PINs mais longos, como de 6 ou 8 dígitos, para aumentar a segurança.

Quando um PIN é enviado para um servidor de autenticação, é crucial garantir que essa transmissão ocorra por um canal seguro por meio de métodos apresentados no tópico 5.3.4 para proteger contra interceptação por atacantes. Além disso, tanto no lado do cliente quanto no servidor, o PIN deve ser armazenado de maneira segura para evitar

acesso não autorizado. Essa senha nunca deve ser armazenada ou manipulada em texto claro, pode ser utilizado Hash Criptográfico (como visto no tópico 5.3.2.3), e devem ser utilizados mecanismos seguros de armazenamento e autenticação, como a API Credential Manager e o Firebase, que oferece suporte a vários métodos de login e autenticação, como nome de usuário e senha, chaves de acesso, entre outros métodos de maneira segura, simplificando assim a integração para os desenvolvedores.

```
1     private FirebaseAuth mAuth;
2
3     mAuth = FirebaseAuth.getInstance();
4
5     FirebaseUser currentUser = mAuth.getCurrentUser();
6     updateUI(currentUser);
7
8     mAuth.signInWithCustomToken(PIN)
9         .addOnCompleteListener(this, new OnCompleteListener<
              AuthResult>() {
10            @Override
11            public void onComplete(@NonNull Task<AuthResult> task
                  ) {
12                if (task.isSuccessful()) {
13                    FirebaseUser user = mAuth.getCurrentUser();
14                    updateUI(user);
15                } else {
16                    // If sign in fails, display a message to the
                          user.
17                    Toast.makeText(CustomAuthActivity.this, "
                          Authentication failed.",
18                            Toast.LENGTH_SHORT).show();
19                    updateUI(null);
20                }
21            }
22        });
```

Listing 5.8 – Autenticação por Pin utilizando firebase em Java

Já na autenticação por biometria em aplicativos é feita utilizando os dados biométricos do usuário por meio do leitor de digital ou reconhecimento facial do dispositivo. Como a autenticação é local e o provedor não tem a digital salva em seu banco de dados, a autenticação deve ser feita de maneira parecida com a de bloqueio de tela, visto que todas as digitais registradas no celular, são validadas. Dessa forma, o Android usa um componente interno para se conectar a biblioteca "Biometric"e ao hardware de impressão

digital e por meio deles validar as informações biométricas lidas no momento da ação. Existem ainda componentes que fornecem criptografia com suporte de hardware para o armazenamento seguro da digital no dispositivo. Com isso, assim deve ser feita a validação das impressões digitais em uma funcionalidade da aplicação ou até de um login:

```
1     private Executor executor;
2     private BiometricPrompt biometricPrompt;
3     private BiometricPrompt.PromptInfo promptInfo;
4
5     @Override
6     protected void onCreate(Bundle savedInstanceState) {
7         super.onCreate(savedInstanceState);
8         setContentView(R.layout.activity_login);
9         executor = ContextCompat.getMainExecutor(this);
10        biometricPrompt = new BiometricPrompt(MainActivity.this,
11                executor, new BiometricPrompt.
                      AuthenticationCallback() {
12            @Override
13            public void onAuthenticationError(int errorCode,
14                    @NonNull CharSequence errString) {
15                super.onAuthenticationError(errorCode, errString)
                      ;
16                Toast.makeText(getApplicationContext(),
17                    "Authentication error: " + errString, Toast.
                          LENGTH_SHORT)
18                    .show();
19            }
20
21            @Override
22            public void onAuthenticationSucceeded(
23                    @NonNull BiometricPrompt.AuthenticationResult
                          result) {
24                super.onAuthenticationSucceeded(result);
25                Toast.makeText(getApplicationContext(),
26                    "Authentication succeeded!", Toast.
                          LENGTH_SHORT).show();
27            }
28
29            @Override
30            public void onAuthenticationFailed() {
31                super.onAuthenticationFailed();
```

```
32                 Toast.makeText(getApplicationContext(), "
                      Authentication failed",
33                     Toast.LENGTH_SHORT)
34                     .show();
35             }
36         });
37
38         promptInfo = new BiometricPrompt.PromptInfo.Builder()
39                 .setTitle("Biometric login for my app")
40                 .setSubtitle("Log in using your biometric
                      credential")
41                 .setNegativeButtonText("Use account password")
42                 .build();
43
44
45         Button biometricLoginButton = findViewById(R.id.
              biometric_login);
46         biometricLoginButton.setOnClickListener(view -> {
47                 biometricPrompt.authenticate(promptInfo);
48         });
49     }
```

Listing 5.9 – Autenticação por digital em Java

5.3.3.2 Autenticação de usuário

Ao falar em autenticação de usuário, os principais método a ser utilizado são o login e senha e, como autenticação de dois fatores, o TOTP.

O login e senha deve funcionar de maneira semelhante ao PIN, com os dados e verificações sendo feitos no servidor e enviados por um canal seguro de comunicação.

```
1     private FirebaseAuth mAuth;
2
3     mAuth = FirebaseAuth.getInstance();
4
5     FirebaseUser currentUser = mAuth.getCurrentUser();
6     if(currentUser != null){
7         reload();
8     }
9
10    mAuth.signInWithEmailAndPassword(email, password)
```

```
11          .addOnCompleteListener(this, new OnCompleteListener<
                AuthResult>() {
12              @Override
13              public void onComplete(@NonNull Task<AuthResult> task
                    ) {
14                  if (task.isSuccessful()) {
15                      Log.d(TAG, "signInWithEmail:success");
16                      FirebaseUser user = mAuth.getCurrentUser();
17                      updateUI(user);
18                  } else {
19                      Toast.makeText(EmailPasswordActivity.this, "
                            Authentication failed.",
20                              Toast.LENGTH_SHORT).show();
21                      updateUI(null);
22                  }
23              }
24          });
```

Listing 5.10 – Autenticação por digital em Java

Já o TOTP, é um algoritmo de senha descartável baseado em tempo, que utiliza uma senha de uso único, gerada com dois parâmetros criptografados juntos. Nesse caso, uma chave secreta compartilhada e uma variável tempo são criptografados por uma função hash. Uma credencial comprometida é válida apenas por um tempo limitado, normalmente expiram após 30, 60, 120 ou 240 segundos. Devido à curta janela de tempo em que os códigos TOTP são válidos, os invasores enfrentam alguns desafios ao realizar ataques a este método. As credenciais TOTP também são baseadas em um segredo compartilhado conhecido tanto pelo cliente quanto pelo servidor. Um invasor com acesso a esse segredo compartilhado pode gerar novos códigos TOTP válidos de maneira indiscriminada, o que pode ser um problema específico se houver violação em um possível banco de dados de autenticação. Logo, o armazenamento é algo que deve ser feito com cuidado. Os serviços do Firebase também oferecem suporte para o uso de autenticação por dois fatores de maneira segura.

```
1       when (exception.resolver.hints[selectedIndex].factorId) {
2           TotpMultiFactorGenerator.FACTOR_ID -> {
3               val otpFromAuthenticator = // OTP escrito pelo
                    usuário.
4               val assertion = TotpMultiFactorGenerator.
                    getAssertionForSignIn(
5                   exception.resolver.hints[selectedIndex].uid,
6                   otpFromAuthenticator
```

```
7               )
8               exception.resolver.resolveSignIn(assertion)
9                   .addOnSuccessListener { result ->
10                      // Successfully signed in!
11                      Log.d(TAG, "signInWithTOTP:success");
12                  }
13                  .addOnFailureListener { resolveError ->
14                      Toast.makeText(TOTPActivity.this, "Invalid or
                            expired OTP.",
15                                  Toast.LENGTH_SHORT).show();
16                  }
17          }
18          PhoneMultiFactorGenerator.FACTOR_ID -> {
19              // Handle SMS second factor.
20          }
21      }
```

Listing 5.11 – Autenticação por TOTP Utilizando Firebase

5.3.4 Segurança de redes

Rede de computadores ou redes de dados, na informática e na telecomunicação é um conjunto de dois ou mais dispositivos eletrônicos de computação interligados por um sistema de comunicação digital, guiados por um conjunto de regras para compartilhar entre si informação, serviços e recursos físicos e lógicos.

A segurança de rede consiste na provisão e políticas adotadas pelo administrador de rede para prevenir e monitorar o acesso não autorizado, uso incorreto, modificação ou negação da rede de computadores e dos seus recursos associados.

5.3.4.1 Rede IP

A rede do Android não é muito diferente de outros ambientes Linux. A principal consideração é garantir que os protocolos apropriados sejam usados para dados sensíveis, como o HTTPS para o tráfego seguro na Web. O HTTPS é a versão do protocolo HTTP com uma camada de criptografia, o TLS ou SSL.

O Transport Layer Security ou TLS é um protocolo feito para garantir segurança nas comunicações em uma rede de computadores. Ele usa vários tipos de criptografia citados em 5.3.2, cada uma com seu papel específico. Essa camada adicional, permite que as informações sejam transmitidas através de uma conexão que é totalmente criptografada

e que a autenticidade do servidor e do cliente sejam verificadas através de certificados digitais.

A comunicação utilizando esse protocolo pode ser facilmente implementada usando a classe SSLSocket.

```
1    SSLSocketFactory socketFactory;
2    SSLSocket socket;
3    socketFactory = (SSLSocketFactory) SSLSocketFactory.
        getDefault();
4    try {
5        socket = (SSLSocket) socketFactory.createSocket(IP, Porta
            );
6        System.out.println("Connected!");
7    } catch (IOException e) {
8        e.printStackTrace();
9    }
```

Listing 5.12 – Conexão criptografada com SSLSocket

5.3.4.2 Rede de telefonia

A rede de telefonia móvel celular é uma rede de telecomunicações projetada para o provisionamento de serviços de telefonia móvel, ou seja, para a comunicação entre uma ou mais estações móveis. O protocolo do serviço de mensagens curtas (SMS) foi projetado principalmente para comunicação entre usuários e não é adequado para apps que querem transferir dados. Devido às limitações do SMS, é recomendado o uso de redes IP no envio de dados de um servidor para a aplicação no dispositivo do usuário.

Ele não é criptografado nem fortemente autenticado na rede ou no dispositivo. Assim, todo receptor de SMS precisa esperar que a mensagem tenha sido enviada ao seu dispositivo por um usuário malicioso. Por conta disso, não se deve usar dados SMS não autenticados para executar comandos essenciais, além de o SMS pode estar sujeito a spoofing e interceptação na rede. No próprio dispositivo Android, as mensagens SMS são transmitidas como intents de transmissão, podendo ser lidas ou capturadas por outros aplicativos que tenham a permissão READ_SMS.

5.4 Processo de desenvolvimento e atualização

O processo de desenvolvimento e atualização de aplicações bancárias no Android deve ser cuidadosamente planejado para garantir a máxima segurança e eficiência. Desde

o início do ciclo de vida do software, é essencial implementar uma abordagem de desenvolvimento seguro. Isso inclui incorporar técnicas de segurança durante o processo de planejamento e design, como estabelecer requisitos de segurança, realizar análises de ameaças e construir uma arquitetura sólida que leve em consideração elementos como criptografia, autenticação e autorização. A automação de testes de segurança e revisões de código frequentes facilitam a identificação e correção de vulnerabilidades durante o desenvolvimento. Ferramentas de análise de código estática e dinâmica devem ser utilizadas para detectar potenciais falhas de segurança, enquanto testes de penetração simulam ataques reais para avaliar a resiliência da aplicação.

Além disso, os métodos de integração contínua e entrega contínua (CI/CD) são sugeridos para garantir que o código seja regularmente testado e validado antes de ser implementado na produção. Essas técnicas reduzem a janela de vulnerabilidade, permitindo a detecção de problemas rápida e a aplicação rápida de correções. A fase de atualização é igualmente importante, especialmente devido à natureza dinâmica das ameaças cibernéticas. Para manter a aplicação segura contra novas vulnerabilidades, é fundamental mantê-la atualizada com as atualizações de segurança mais recentes do Android e de bibliotecas de terceiros. O monitoramento contínuo da aplicação em produção, com o uso de ferramentas de detecção e resposta a incidentes, é essencial para identificar e reduzir rapidamente os riscos que surgem.

Adicionalmente, a educação e o treinamento contínuos dos desenvolvedores em práticas de segurança são essenciais para manter uma postura de segurança proativa. Workshops, cursos e certificações podem ajudar a equipe a se manter atualizada sobre as últimas ameaças e técnicas de mitigação.

Por fim, uma comunicação transparente com os usuários sobre as atualizações de segurança, boas práticas de uso e ataques de engenharia social fortalece a confiança com a empresa e o compromisso do indivíduo com a segurança.

Capítulo 6: Discussões

A análise dos componentes de segurança em aplicações bancárias no Android, conforme detalhado nos capítulos 3 e 5, revela uma série de pontos críticos que devem ser cuidadosamente considerados para garantir a proteção dos dados dos usuários e a integridade das transações financeiras.

Os achados desta análise corroboram com o referencial teórico discutido anteriormente, especialmente com as diretrizes e recomendações da OWASP Mobile Top 10 descritas no tópico 2.3.1 que engloba a maioria das ameaças citadas no presente trabalho. A importância dos métodos de segurança descritos são questões enfatizadas tanto na literatura quanto nos resultados deste estudo.

O malware surge como um risco significativo para aplicativos bancários no Android, conforme indicado pelas descobertas. Essa forma de software malicioso possui a capacidade de se infiltrar nos dispositivos dos usuários por meio de aplicativos falsificados ou comprometidos, com o objetivo de roubar dados confidenciais, como credenciais bancárias e informações pessoais. A necessidade de medidas de segurança robustas, incluindo a utilização correta das proteções do Android, é ressaltada pela prevalência de malware.

Outra ameaça crítica é representada pelos ataques de autenticação. A análise mostrou que cibercriminosos frequentemente tentam comprometer o procedimento de login do usuário para obter acesso não autorizado às suas contas. A incorporação da autenticação multifatorial (MFA) apresenta uma solução viável para esse tipo de ataque, introduzindo camadas adicionais de segurança além das senhas convencionais. O uso da biometria e dos códigos de uso único baseado em tempo (TOTP) constituem estratégias eficazes que podem melhorar substancialmente a segurança das autenticações.

Métodos de criptografia inadequados podem resultar na exposição de dados confidenciais à interceptação e decodificação por entidades maliciosas, conforme revelado pela análise. Dessa forma, a inadequação da criptografia se destaca como um problema notável. A adoção de algoritmos contemporâneos e rigorosamente testados, como o AES-256 para criptografia simétrica, juntamente com o gerenciamento seguro de chaves, é fundamental

para mitigar esse risco. O emprego da Assinatura digital com a criptografia assimétrica e do Hash criptográfico garante a preservação da integridade e autenticidade dos dados durante toda a transmissão e armazenamento.

A ameaça contínua de ataques de rede contra aplicativos bancários móveis também é evidente. A potencial interceptação e manipulação da comunicação, advinda do uso móvel dos dispositivos analisados, entre os usuários e o servidor do banco podem levar a graves perdas. Para combater essas ameaças, a adoção de protocolos de comunicação seguros como TLS (Transport Layer Security), a validação meticulosa de certificados e a integração de medidas complementares são defendidas como melhores práticas.

A incidência de muitas ameaças indicam que a segurança das aplicações bancárias no Android ainda enfrenta desafios significativos. A sofisticação crescente dos ataques requer soluções inovadoras e uma abordagem proativa à segurança. Uma direção futura para o tema é a combinação de tecnologias inovadoras, como inteligência artificial (OGUNTIMILEHIN et al., 2022), IOT (CHAITHANYA et al., 2021) e a implementação de novas formas de autenticação (HUSSEIN, 2022), e como elas podem fornecer uma defesa eficaz contra essas ameaças.

Por fim, as descobertas desta monografia têm implicações práticas significativas para desenvolvedores de aplicativos bancários, instituições financeiras e especialistas em cibersegurança. A implementação das práticas robustas de segurança baseadas nos resultados deste estudo podem gerar sérios impactos positivos no desenvolvimento de aplicações bancárias no Android. Dentre elas o aumento da segurança das aplicações e da confiança dos clientes, com a utilização das recomendações desta pesquisa para implementar medidas de segurança avançadas; a redução de riscos e custos, com a proteção da reputação da instituição financeira associado a diminuição dos riscos, violações de segurança e ataques cibernéticos; e melhores adaptações à regulamentações de segurança, com o auxílio para instituições financeiras a estar em conformidade com regulamentações rigorosas de proteção de dados.

Capítulo 7:
Conclusão

Esta monografia examinou minuciosamente a segurança dos aplicativos bancários no sistema operacional Android, com foco nos principais desafios, ameaças, melhores práticas e recomendações para mitigação. Verificou-se que garantir a segurança em aplicativos bancários móveis é uma área complexa que exige uma abordagem multifacetada para proteger os dados do usuário e manter a integridade das transações financeiras.

Garantir a segurança dos aplicativos bancários Android exige uma abordagem holística que combine tecnologias avançadas, práticas de desenvolvimento seguro e vigilância contínua contra novas ameaças. A colaboração entre desenvolvedores, instituições financeiras e especialistas em segurança é essencial para estabelecer um ambiente seguro e confiável para os usuários.

As principais contribuições desta pesquisa estão na base de dados teórica, que apontam a Comunicação entre processos, Criptografia, Autenticação e Redes como os pontos críticos das aplicações bancárias; e nas recomendações práticas em cada área fornecidas para aprimorar a segurança dos aplicativos bancários Android. A pesquisa e o desenvolvimento contínuos de novas tecnologias de segurança também são cruciais para lidar com ameaças emergentes e aprimorar a segurança no campo dos aplicativos bancários móveis. Ao implementar essas metodologias e manter uma postura proativa em relação à segurança, desenvolvedores e instituições financeiras podem estabelecer um ambiente seguro para seus clientes, aumentando assim a confiança nas plataformas bancárias móveis e protegendo informações confidenciais dos riscos cibernéticos em constante mudança.

Referências

ALZOUBI, H. M. et al. Cyber security threats on digital banking. In: *2022 1st International Conference on AI in Cybersecurity (ICAIC)*. [S.l.: s.n.], 2022. p. 1–4. Citado na página 24.

ARANHA, D. F.; CRUZ, R. J. Análise de segurança em aplicativos bancários na plataforma android. In: . [s.n.], 2015. Disponível em: <https://proceedings.science/unicamp-pibic/pibic-2015/trabalhos/analise-de-seguranca-em-aplicativos-bancarios-na-plataforma-android?lang=pt-br>. Citado 2 vezes nas páginas 7 e 8.

BILAL, M.; SANKAR, G. Trust security issues in mobile banking and its effect on customers. *International Research Journal of Modernization in Engineering Technology and Science*, 2023. Citado na página 25.

BOITAN, I. A. Cyber security challenges through the lens of financial industry. *Proceedings of The 2nd International Conference on Advanced Research in Management, Business and Finance*, 2019. Disponível em: <https://api.semanticscholar.org/CorpusID:227317657>. Citado na página 25.

CHAITHANYA, J. K. et al. Design and development of virtual banking using internet of things. In: *2021 6th International Conference on Communication and Electronics Systems (ICCES)*. [S.l.: s.n.], 2021. p. 586–592. Citado na página 48.

Chandra sekhar; KUMAR, M. An overview of cyber security in digital banking sector. *East Asian Journal of Multidisciplinary Research*, PT Formosa Cendekia Global, v. 2, n. 1, p. 43–52, jan. 2023. Citado na página 23.

CHEN, S. et al. An empirical assessment of security risks of global android banking apps. In: *2020 IEEE/ACM 42nd International Conference on Software Engineering (ICSE)*. [S.l.: s.n.], 2020. p. 1310–1322. Citado na página 21.

DAREM, A. A. et al. Cyber threats classifications and countermeasures in banking and financial sector. *IEEE Access*, v. 11, p. 125138–125158, 2023. Citado na página 22.

DATTA, P. et al. Security and issues of m-banking: A technical report. In: *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. [S.l.: s.n.], 2020. p. 1115–1118. Citado na página 26.

DELOITTE. *Pesquisa FEBRABAN de Tecnologia Bancária*. Rio de Janeiro, 2021. 70 p. Citado 3 vezes nas páginas 5, 6 e 7.

FALADE, P. V.; OGUNDELE, G. B. *Vulnerability Analysis of Digital Banks' Mobile Applications*. 2023. Citado na página 23.

GARG, S.; BALIYAN, N. *Mobile OS vulnerabilities*. London, England: CRC Press, 2023. Citado na página 15.

HASSAN, M.; SHUKUR, Z.; MOHD, M. A penetration testing on malaysia popular e-wallets and m-banking apps. *International Journal of Advanced Computer Science and Applications*, v. 13, 06 2022. Citado na página 26.

HINTZBERGEN, J. et al. *Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002*. [S.l.]: Brasport, 2018. Citado 3 vezes nas páginas 11, 12 e 13.

HUSSEIN, O. A proposed anti-fraud authentication approach for mobile banking apps. In: *2022 4th Novel Intelligent and Leading Emerging Sciences Conference (NILES)*. [S.l.: s.n.], 2022. p. 56–61. Citado na página 48.

ISLAM, M. S. Systematic Literature Review : Security Challenges of Mobile Banking and Payments System. *International Journal of u- and e- Service, Science and Technology*, Science I& Engineering Research Support Center, Republic of Korea(IJUNESST), 7, p. 107–116, 2014. Disponível em: <https://www.earticle.net/Article/A237109>. Citado na página 8.

LAKATOS, E. M.; MARCONI, M. de A. *Fundamentos de Metodologia Científica*. [S.l.: s.n.], 2021. Citado na página 27.

LIU, W.; WANG, X.; PENG, W. State of the art: Secure mobile payment. *IEEE Access*, v. 8, p. 13898–13914, 2020. Citado na página 25.

LLC, G. *Ferramentas para desenvolvedores de apps para dispositivos móveis Android*. 2024. Disponível em: <https://developer.android.com/>. Citado 4 vezes nas páginas 13, 14, 15 e 31.

MARTINS, G. de A.; PINTO, R. L. *Manual para elaboração de trabalhos acadêmicos*. [S.l.: s.n.], 2001. Citado na página 27.

OGUNTIMILEHIN, A. et al. Mobile banking transaction authentication using deep learning. In: *2022 5th Information Technology for Education and Development (ITED)*. [S.l.: s.n.], 2022. p. 1–7. Citado na página 48.

OWASP. *OWASP Mobile Top 10*. 2023. Disponível em: <https://owasp.org/www-project-mobile-top-10/>. Citado 2 vezes nas páginas 15 e 16.

S., A.; SALEH, Z. Community perception of the security and acceptance of mobile banking services in bahrain: An empirical study. *International Journal of Advanced Computer Science and Applications*, v. 6, 09 2015. Citado 2 vezes nas páginas 21 e 30.

SINGHAL, N.; NATH, V.; GOEL, A. *Mobile banking: An introduction*. [S.l.: s.n.], 2019. Citado na página 5.

STANIKZAI, A. Q.; SHAH, M. A. Evaluation of cyber security threats in banking systems. In: *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*. [S.l.: s.n.], 2021. p. 1–4. Citado na página 24.

TÉLLEZ, J.; ZEADALLY, S. *Mobile payment systems*. 1. ed. Basel, Switzerland: Springer International Publishing, 2017. (Computer Communications and Networks). Citado na página 5.

UBALDO, A. L. V. et al. Information security in the banking sector: A systematic literature review on current trends, issues, and challenges. *Int. J. Saf. Secur. Eng.*, International Information and Engineering Technology Association, v. 13, n. 1, p. 97–106, fev. 2023. Citado na página 22.

WANG, Y.; HAHN, C.; SUTRAVE, K. Mobile payment security, threats, and challenges. In: *2016 Second International Conference on Mobile and Secure Services (MobiSecServ)*. [S.l.: s.n.], 2016. p. 1–5. Citado 2 vezes nas páginas 8 e 26.

WODO, W.; STYGAR, D.; BŁAŚKIEWICZ, P. Security issues of electronic and mobile banking. In: *Proceedings of the 18th International Conference on Security and Cryptography*. [S.l.]: SCITEPRESS - Science and Technology Publications, 2021. Citado na página 24.

YILDIRIM, N.; VAROL, A. A research on security vulnerabilities in online and mobile banking systems. In: *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*. [S.l.: s.n.], 2019. p. 1–5. Citado na página 21.