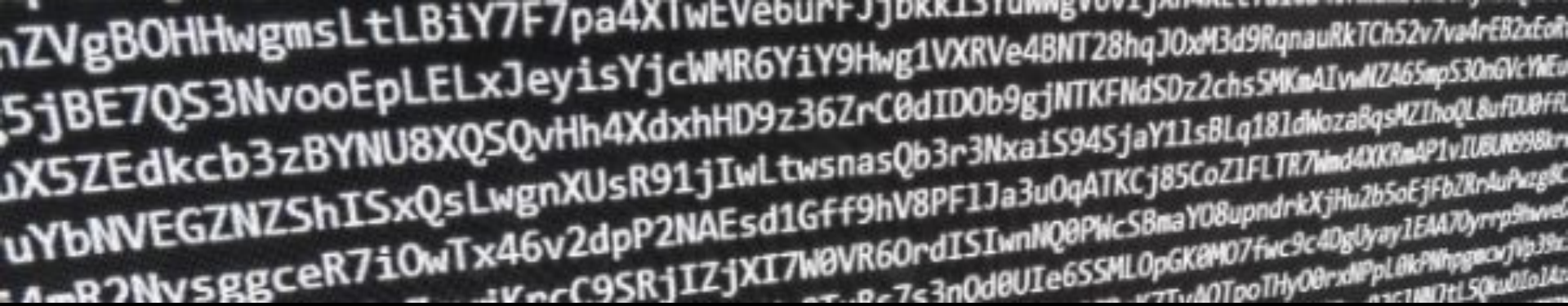


Um modelo de requisitos de segurança para aplicações bancárias no Android

—

José Lucio C. Azevedo

Introdução

- Contexto
- Problemática
- Hipótese
- Objetivos
- Justificativa
- Resultados

Contexto

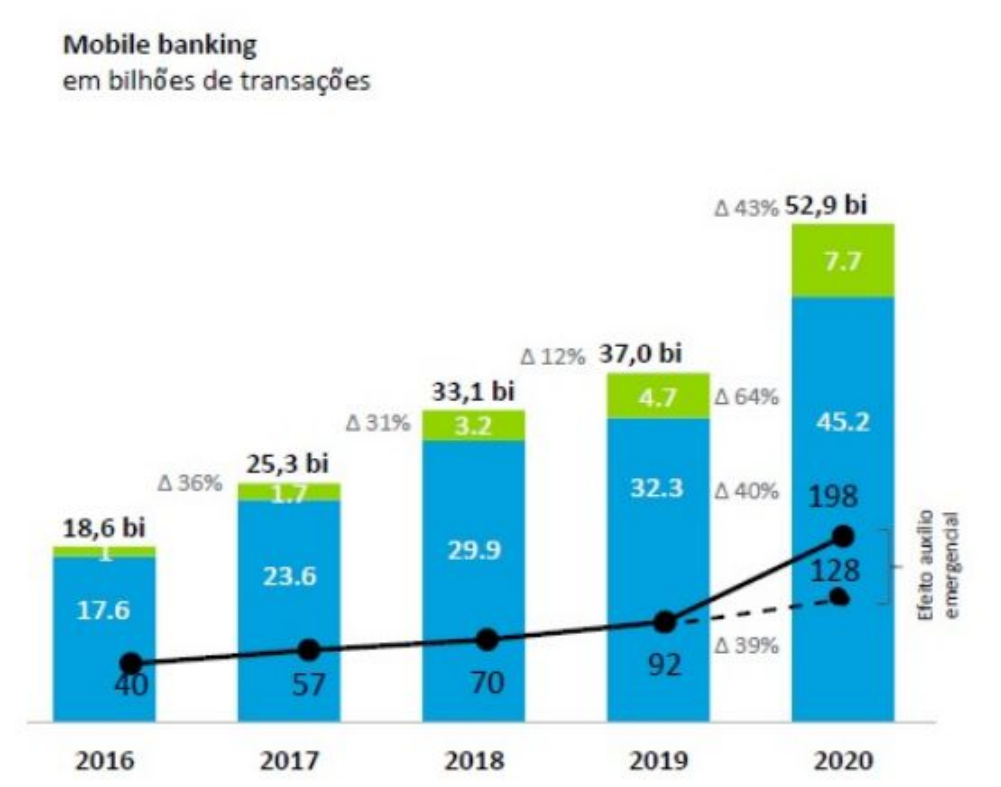
Desde os tempos antigos os métodos de pagamento e manipulação de dinheiro vêm mudando de maneira constante, por conta do crescimento da complexidade da sociedade e novas tecnologias desenvolvidas.

1. Escambo
2. Moeda
3. Cartão bancários
4. Aplicações bancárias

Aplicações bancárias

Tendência

Uma pesquisa sobre tecnologia bancária revelou um aumento de 20% no número de transações realizadas por dispositivos móveis de 2019 para 2020.



Problemas de segurança

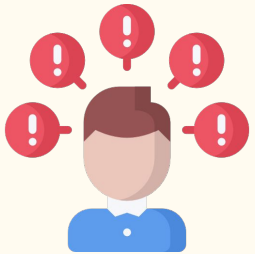
Em 2015, dois pesquisadores da Unicamp realizaram um estudo para identificar deficiências e fragilidades nos aplicativos de bancos brasileiros para android.

	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

Problemática

As aplicações bancárias são alvos atraentes para cibercriminosos devido à quantidade significativa de informações sensíveis que manipulam. Essas plataformas enfrentam dificuldades como:

- A complexidade do ecossistema e ameaças móveis
- Práticas inadequadas de desenvolvimento
- A crescente sofisticação dos ataques cibernéticos



Hipótese

A proposta de um modelo de requisitos de segurança, com base em uma revisão da literatura ressaltando ameaças e remediações eficazes, pode estabelecer diretrizes claras para o desenvolvimento seguro dessas aplicações no Android, abordando aspectos e cenários específicos do meio financeiro digital.

Objetivos

O objetivo geral deste presente trabalho é propor um modelo de segurança para plataformas bancárias no Android, que seja capaz de mitigar os principais riscos e ameaças encontrados no cenário.

Os objetivos específicos incluem:

- Realizar uma pesquisa de revisão visando os principais pontos críticos de segurança.
- Propor um modelo de requisitos de segurança.
- Avaliar a eficácia e a viabilidade do modelo de requisitos de segurança proposto.

Justificativa

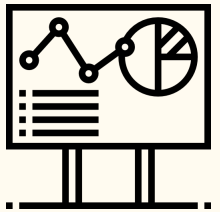
A justificativa para este trabalho reside na necessidade premente de combater essas vulnerabilidades. A segurança nos aplicativos bancários é fundamental para:

- Proteger as informações confidenciais e ativos do usuário
- Manter a integridade e a confiabilidade da infraestrutura financeira digital.

Dada a crescente dependência das tecnologias móveis, as violações de segurança têm o potencial de levar a perdas financeiras significativas e manchar a reputação das instituições envolvidas.

Resultados esperados

Com a conclusão deste trabalho, espera-se obter um modelo de requisitos de segurança para desenvolvedores de aplicações bancárias e com isso a minimização de riscos e ameaças na implementação e uso de aplicações bancárias, promovendo uma cultura de segurança mais sólida e específica para o meio.



Referencial teórico

- Segurança da informação
- Sistema operacional Android
- Aplicações bancárias
- Engenharia de requisitos

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. Esse objetivo é descrito nos seus pilares principais:

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticidade
- Não-repúdio

Sistema operacional Android

O Android é um sistema operacional de código aberto baseado no kernel Linux, desenvolvido inicialmente pela Android Inc. e adquirido pelo Google em 2005.

- Arquitetura
- Componentes do Android
  - Activity
  - Services
  - Content Providers
  - Broadcast Receivers
- Mecanismos de segurança nativos

Segurança nas aplicações bancárias móveis

Os serviços bancários móveis compartilham a necessidade crítica de segurança da informação com outros sistemas, mas diferem em alguns aspectos de implementação e preocupações específicas.

- Ataques cibernéticos visando recompensa financeira imediata
- Armazenamento de dados sensíveis
- Conformidade com regulamentações

Ameaças e remediações nas aplicações bancárias

A Research on Security Vulnerabilities in Online and Mobile Banking Systems

Nilay YILDIRIM
Dept. of Software Engineering
Firat University
Elazig,Turkey
nilyildirim87@gmail.com

Asaf VAROL
Dept. of Software Engineering
Firat University
Elazig, Turkey
varol.asaf@gmail.com

Information Security in the Banking Sector: A Systematic Literature Review on Current Trends, Issues, and Challenges

Alfredo Leonidas Vasquez Ubaldo[1], Vanessa Yeny Gutierrez Barreto[1], Juan Andres Berrios Albines[1], Laberiano Andrade-Arenas[2], Roberto Santiago Bellido-García[3*]

[1] Facultad de Ingeniería y Negocios, Universidad Privada Norbert Wiener, Lima 15046, Perú
[2] Facultad de Ingeniería, Universidad Tecnológica del Perú, Lima 15046, Perú
[3] Postgraduate School, Universidad San Ignacio de Loyola, Lima 15024, Perú

An Overview of Cyber Security in Digital Banking Sector

S. Chandra Sekhar[1*], Manojkumar Kumar[2]
Sree Vaidyanathan Institute of Management
Corresponding Author: S Chandra Sekhar
chandrasekhar.s@vidyanikethan.edu

Cyber Threats Classifications and Countermeasures in Banking and Financial Sector

ABDULBASIT A. DAREM[1], (Member, IEEE), ASMA A. ALHASHMI[1], TAREQ M. ALKHALDI[2], ABDULLAH M. ALASHJAEE[3], SULTAN M. ALANAZI[1], AND SHOUKI A. EBAD[1]
[1]Department of Computer Science, Northern Border University, Arar 73213, Saudi Arabia
[2]Department of Educational Technologies, Imam Abdulrahman Bin Faisal University, Dammam 34221, Saudi Arabia
[3]Department of Computer Sciences, Faculty of Computing and Information Technology, Northern Border University, Rafha 91911, Saudi Arabia
Corresponding author: Abdulbasit A. Darem (basit.darem@nbu.edu.sa)

This work was supported by the Deanship of Scientific Research, Northern Border University, Arar, Saudi Arabia, under Grant RG-NBU-2022-1724.

NDA Journal of Military Science and Disciplinary Studies
ISSN: 2814-3264
Volume 1, Issue 1, June 2022, pp. 44 - 55

Vulnerability Analysis of Digital Banks' Mobile Applications

***PV Falade, GB Ogundele**
Department of Cyber Security, Nigerian Defence Academy, Kaduna
***Corresponding Email**: pvfalade@nda.edu.ng

An Empirical Assessment of Security Risks of Global Android Banking Apps

Sen Chen[1], Lingling Fan[1], Guozhu Meng[2,3], Ting Su[4], Minhui Xue[5], Yinxing Xue[6]
Yang Liu[1,8], Lihua Xu[7]
[1]Nanyang Technological University, Singapore
[2]SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences, China
[3]School of Cyber Security, University of Chinese Academy of Sciences, China [4]ETH Zurich, Switzerland
[5]The University of Adelaide, Australia [6]University of Science and Technology of China, China
[7]New York University Shanghai, China [8]Zhejiang Sci-Tech University, China
chensen@ntu.edu.sg

PCI DSS

O PCI DSS (Payment Card Industry Data Security Standard) é um conjunto de normas e uma certificação de segurança criada com o objetivo de proteger os dados bancários e de pagamentos.

PCI DSS

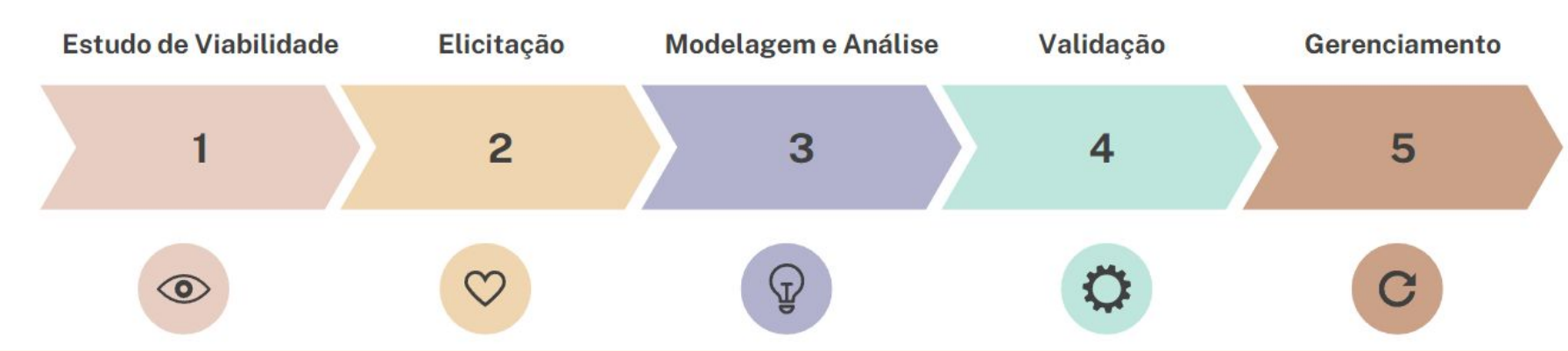
Padrão de Segurança de Dados do PCI - Visão Geral de Alto Nível	
Construir e Manter uma Rede e Sistemas Seguros	**1.** Instalar e Manter Controles de Segurança de Rede. **2.** Aplicar as Configurações de Segurança para Todos os Componentes de Sistema.
Proteger os Dados da Conta	**3.** Proteger os Dados da Conta Armazenados. **4.** Proteger os Dados do Titular do Cartão com Criptografia Forte Durante a Transmissão em Redes Públicas Abertas.
Manter um Programa de Gestão de Vulnerabilidade	**5.** Proteger Todos os Sistemas e Redes de Software Malicioso. **6.** Desenvolver e Manter Sistemas e Software Seguros.
Implementar Medidas Fortes de Controle de Acesso	**7.** Restringir o Acesso aos Componentes de Sistema e aos Dados do Titular do Cartão por Necessidade de Conhecimento do Negócio. **8.** Identificar Usuários e Autenticar o Acesso aos Componentes de Sistema **9.** Restringir o Acesso Físico aos Dados do Titular do Cartão.
Monitorar e Testar as Redes Regularmente	**10.** Registrar e Monitorar Todo o Acesso aos Componentes de Sistema e Dados do Titular do Cartão. **11.** Testar a Segurança de Sistemas e Redes Regularmente.
Manter uma Política de Segurança da Informação	**12.** Apoiar a Segurança da Informação com Políticas e Programas Organizacionais.

Engenharia de requisitos

Os requisitos de um sistema são descrições das funcionalidades que o sistema deve possuir, os serviços que ele oferece e condições ou capacidades que deve ser atendida ou possuídas pelo mesmo.

Fases

A Engenharia de Requisitos envolve várias fases que se repetem em um ciclo contínuo. Estas etapas são continuamente realizadas para analisar os problemas e as necessidades do projeto, oferecendo soluções baseadas nos requisitos definidos.

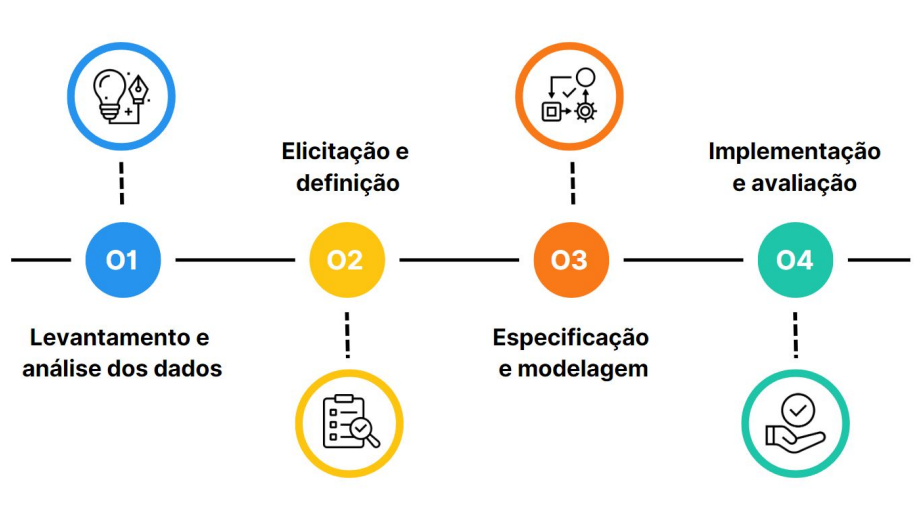


Metodologia do trabalho

- Levantamento e análise
- Elicitação e definição
- Especificação e modelagem
- Implementação e avaliação

Metodologia

Este trabalho se inicia em uma revisão das literaturas para que sirvam de base para as análises. Em seguida, foram realizadas etapas do ciclo de vida da engenharia de requisitos a fim de se obter um modelo de segurança específico.



Levantamento e análise de dados

Para a confecção do trabalho foram utilizados artigos científicos com os seguintes parâmetros:

- Artigos encontrados em plataformas públicas como Google Scholar e IEEE Xplore
- Utilizando a palavras chave “Mobile Banking Security”
- 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?

Após a coleta dos dados, procedeu-se à leitura do material, chegando na compilação das informações mais relevantes e a compreensão e aprofundamento sobre o tema investigado.

Elicitação e definição de requisitos

Com o compilado de informações, foi feita a elicitação dos requisitos utilizando a técnica de caso de uso indevido com os seguintes objetivos:

- Entender e descrever as principais interações maliciosas que podem comprometer o sistema.
- Criar uma base para definir os requisitos de segurança.

Com a identificação dos casos de uso indevidos do sistema, foram definidos requisitos de segurança que especificam controles e mecanismos necessários para mitigar esses riscos associados.

Especificação e modelagem de requisitos

Após a definição dos requisitos de segurança, foi realizada a especificação e modelagem desses requisitos utilizando diagramas UML (Unified Modeling Language), para representar, organizar e comunicar os aspectos estruturais (estáticos) e comportamentais (dinâmicos) do sistema de maneira clara e estruturada.

Foi utilizado o software Visual Paradigm para criar diversos tipos de diagramas:

- Diagramas de Caso de Uso
- Diagramas de Classe
- Diagramas de Sequência

Implementação e avaliação do modelo

A etapa final do processo é um estudo de caso no qual os requisitos de segurança são propostos no ambiente Android, utilizando a aplicação bancária Herd Financial como base. Este estudo de caso nos permitiu:

- Validar a viabilidade técnica em um cenário realista.
- Entender como a implementação dos requisitos atuaria na aplicação.

Além disso, uma avaliação detalhada do modelo de segurança proposto, utilizando como referência a certificação PCI DSS. Este processo de avaliação serve para:

- Validar a eficácia e adequação do modelo no contexto de aplicações bancárias.
- Identificar seus pontos fortes e lacunas.

Análise de requisitos

- Elicitação
- Definição
- Especificação
- Modelagem

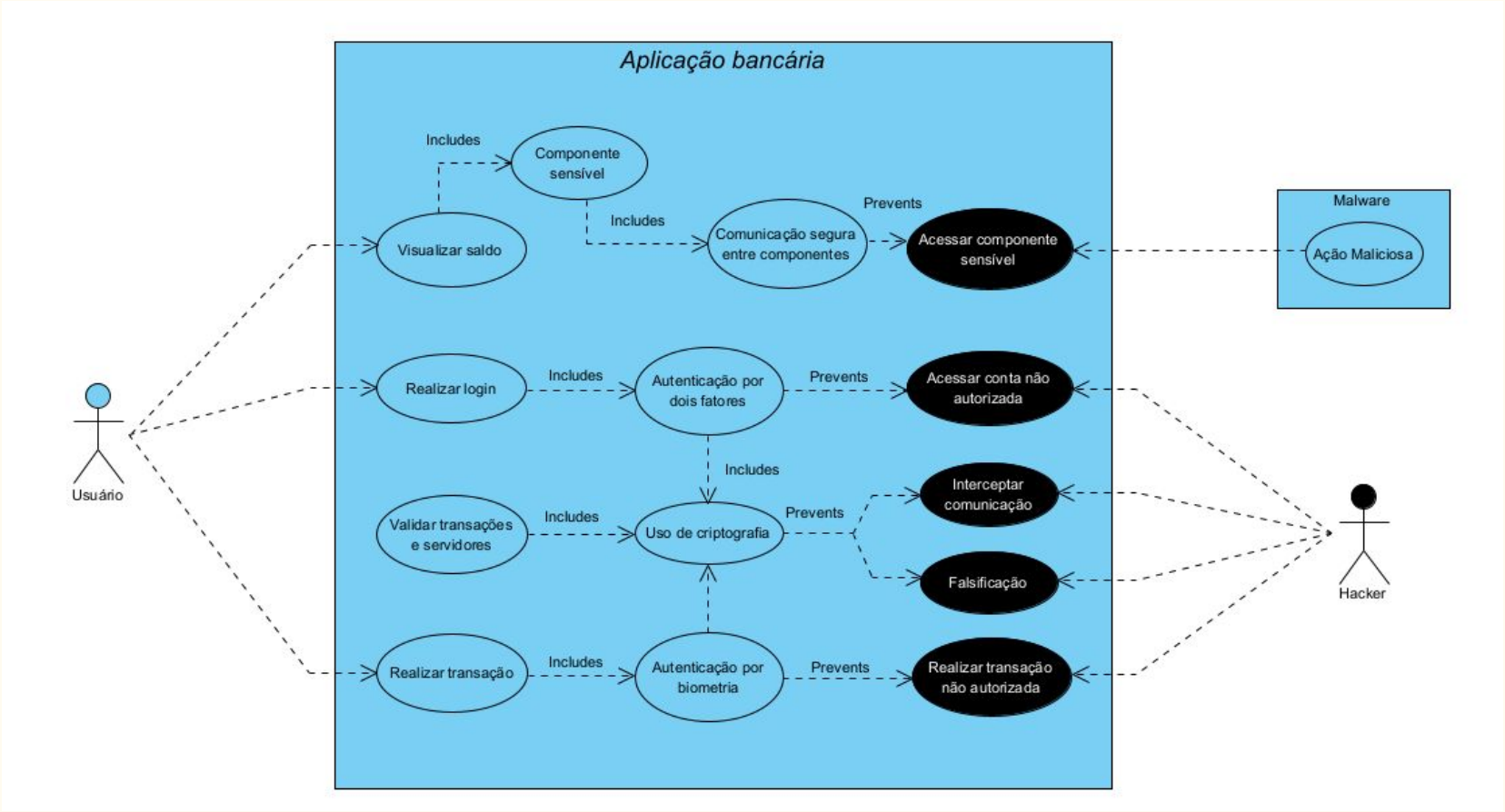
Elicitação de requisitos

A compreensão dos 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.

Os pontos críticos encontrados na literatura foram:

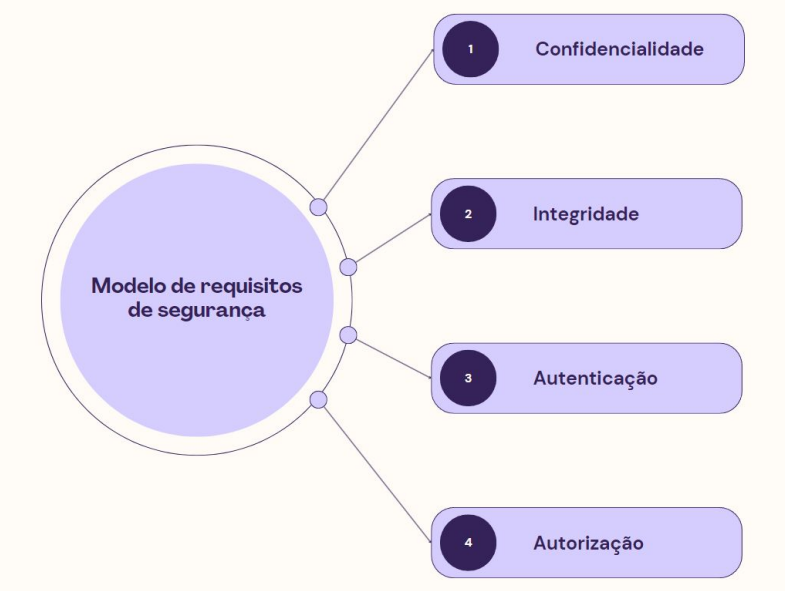
- Malwares
- Falhas de autenticação
- Problemas na criptografia
- Vulnerabilidades de rede

Casos de uso indevido



Definição de requisitos

A partir da análise do cenários de ameaças, foi realizada a definição dos requisitos de segurança necessários para mitigar os riscos associados. Esses requisitos foram divididos em áreas, como visto abaixo:

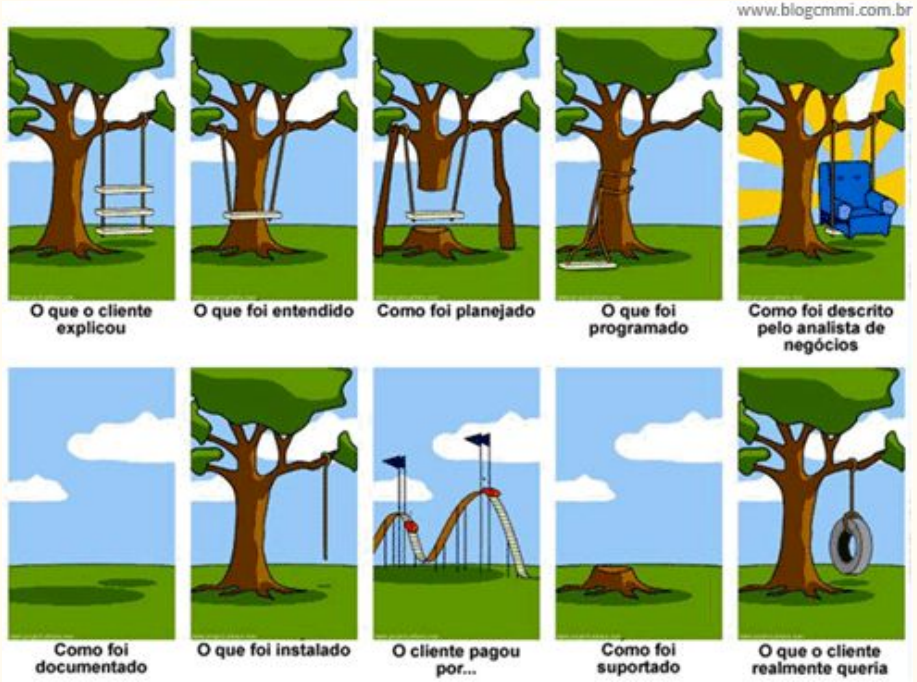


Requisitos do modelo

- Requisitos de confidencialidade
  1. O sistema deverá utilizar criptografia para armazenar senhas e chaves.
  2. A aplicação deverá utilizar TLS para realizar a comunicação com o servidor.
- Requisitos de integridade
  3. O sistema deverá armazenar o Hash de cada transação.
  4. O sistema deverá armazenar a assinatura digital do pagador em cada transação.
  5. O sistema deverá reconhecer apenas o certificado fixado para a comunicação.
- Requisitos de autenticação
  6. O acesso ao sistema deverá ser feito utilizando autenticação de dois fatores (2FA).
  7. O sistema deverá exigir Pin ou biometria para a realização de transações e pagamentos.
- Requisitos de autorização
  8. O sistema não deve exportar componentes que não exigem interação externa.
  9. O sistema deve exigir permissões para acessar os componentes exportados.
  10. O sistema deve validar de intents recebidas nos componentes exportados.

Especificação de requisitos

A especificação dos requisitos é um processo crítico que envolve o definição clara, detalhada e estruturada dos requisitos de segurança definidos anteriormente.



Especificação de requisitos

6. O acesso ao sistema deverá ser feito utilizando autenticação de dois fatores (2FA).

6.1 Exibir a interface de login para o usuário.

6.2 Solicitar nome de usuário e senha.

6.3 Verificar usuário e senha cadastrada.

6.4 Enviar senha de uso único baseada em tempo ao número cadastrado por SMS.

6.5 Solicitar a senha de uso.

6.6 Verificar senha.

6.7 Liberar o acesso ao perfil de usuário após a validação dos dois fatores bem-sucedida.

6.8 Permitir acesso às funcionalidades do sistema.

6.9 Finalizar processo.

Especificação de requisitos

8. O sistema não deve exportar componentes que não têm interação externa

8.1 Identificar componentes que não necessitam de interação externa.

8.2 Definir como “false” a exportação desses componentes.

8.3 Verificar a configuração de componentes para garantir que não estão exportados indevidamente.

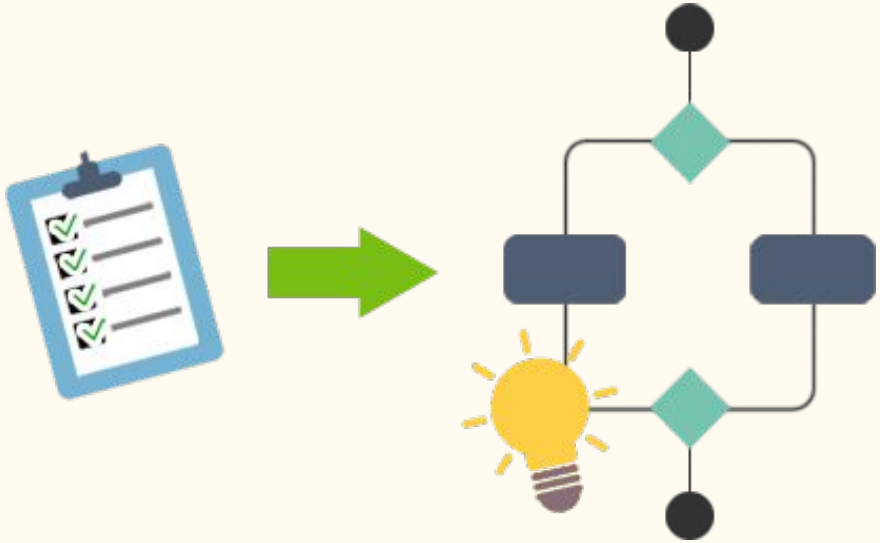
8.4 Monitorar o sistema para identificar tentativas de acesso a componentes não exportados.

8.5 Registrar qualquer tentativa de interação não autorizada para auditoria.

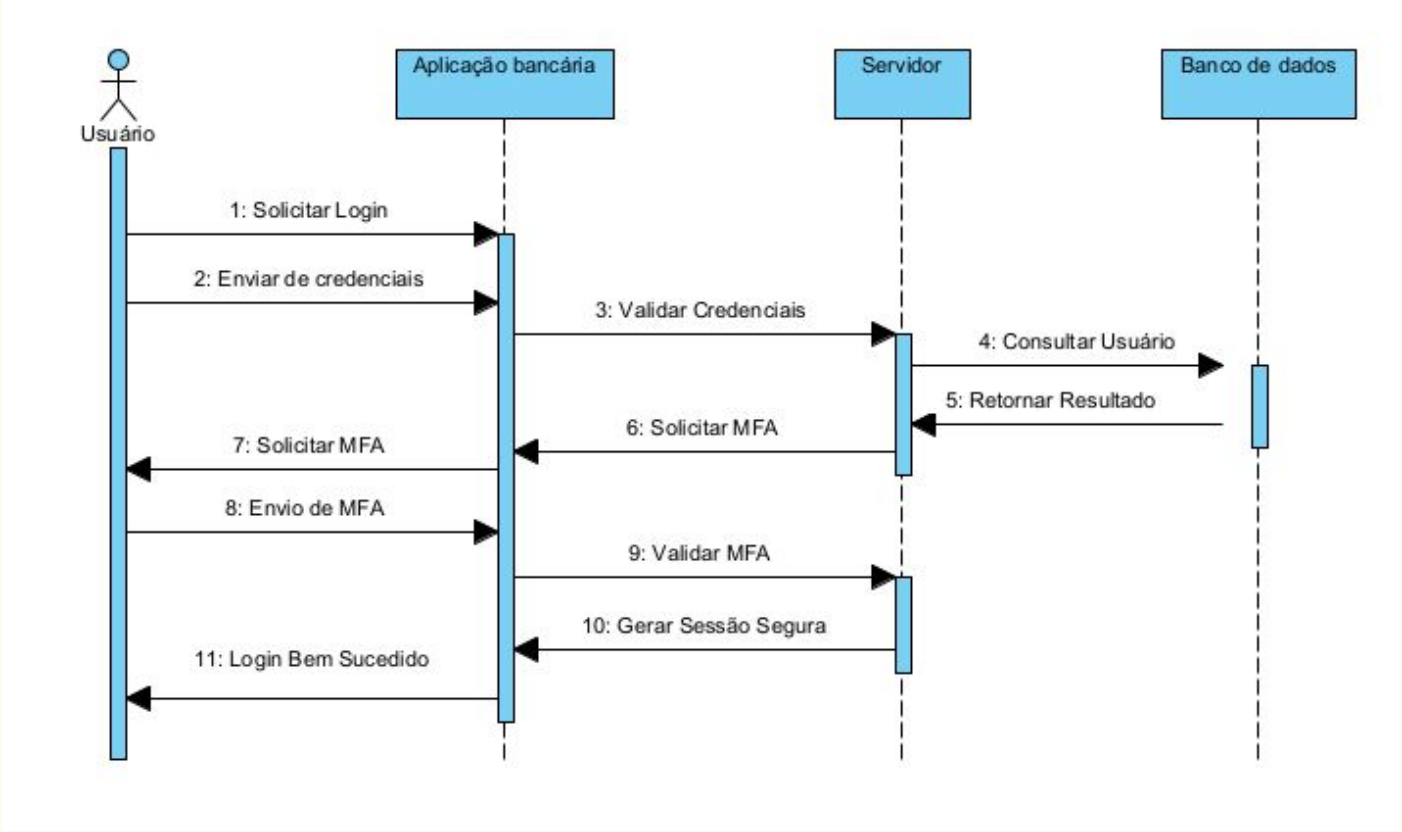
8.6 Encerrar processos que tentem acessar componentes não exportados.

Modelagem de requisitos

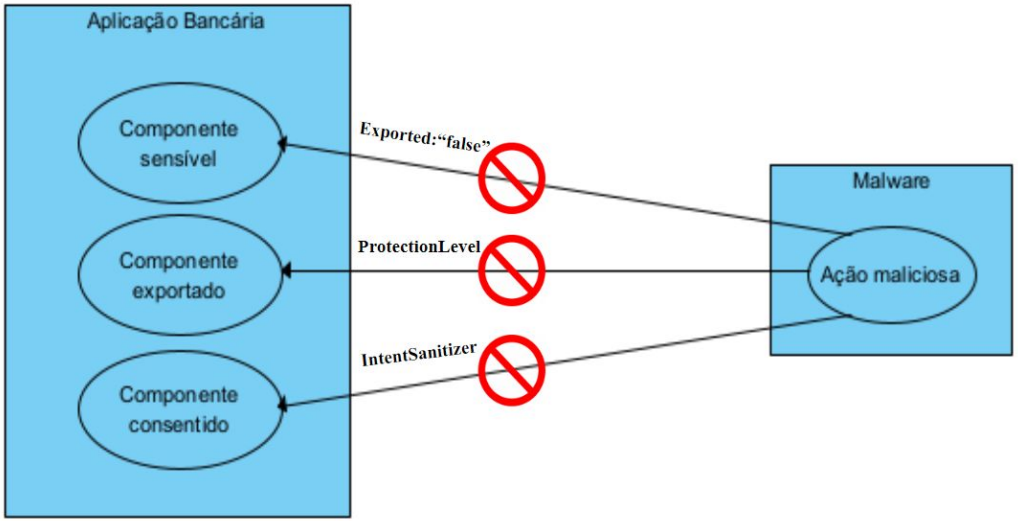
A modelagem de dados e processos é uma fase essencial no desenvolvimento de sistemas, servindo como a base para a construção de soluções tecnológicas que sejam eficientes, escaláveis e alinhadas com os objetivos organizacionais.



6. O acesso ao sistema deverá ser feito utilizando autenticação de dois fatores



8. O sistema não deve exportar componentes que não exigem interação externa.
9. O sistema deve exigir permissões para acessar os componentes exportados.
10. O sistema deve validar de intents recebidas nos componentes exportados.



Implementação e avaliação

- Implementação teórica
- Avaliação de conformidade
- Análise do trabalho

Implementação teórico

Para avaliar a eficácia e viabilidade, analisamos algumas das fragilidades presentes na aplicação Herd Financial e logo após apontamos os requisitos de segurança modelados na etapa anterior capazes de mitigar essas vulnerabilidades, demonstrando exemplos de implementação em Java.

Autenticação simples

Herd Financial inicialmente utilizava um sistema básico de autenticação com senha mostrado sem suporte a autenticação multifatorial (MFA).

Este método simples de autenticação pode ser vulnerável a ataques de força bruta e acessos não autorizados.

6. O acesso ao sistema deverá ser feito utilizando autenticação de dois fatores (2FA).

O modelo recomenda a autenticação multifatorial, adicionando uma camada adicional de segurança ao exigir um segundo fator de autenticação. No caso, um algoritmo de senha descartável baseado em tempo (TOTP).

Autenticação por TOTP Utilizando Firebase

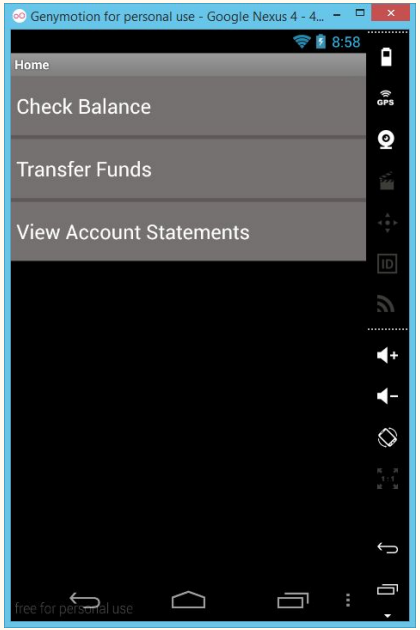
```
when (exception.resolver.hints[selectedIndex].factorId) {
    TotpMultiFactorGenerator.FACTOR_ID -> {
        val otpFromAuthenticator = // OTP escrito pelo
           usuário.
        val assertion = TotpMultiFactorGenerator.
           getAssertionForSignIn(
            exception.resolver.hints[selectedIndex].uid,
            otpFromAuthenticator
        )
        exception.resolver.resolveSignIn(assertion)
            .addOnSuccessListener { result ->
                // Successfully signed in!
                Log.d(TAG, "signInWithTOTP:success");
            }
            .addOnFailureListener { resolveError ->
                Toast.makeText(TOTPActivity.this, "Invalid or
                    expired OTP.",
                        Toast.LENGTH_SHORT).show();
            }
    }
}
```

Componente acessível por malwares

No HerdFinancial, a activity Main (principal) foi exportada e não tem nenhuma permissão personalizada.

O que permite a um malware enviar uma Intent e iniciar a atividade com a conta padrão do sistema.

```
dz> run app.activity.start --component org.owasp.goatdroid.herdfinancial org.owasp.
goatdroid.herdfinancial.activities.Main
```



8. O sistema não deve exportar componentes que não exigem interação externa.
9. O sistema deve exigir permissões para acessar os componentes exportados.
10. O sistema deve validar de intents recebidas nos componentes exportados.

Ao utilizar as configurações corretas e permissões nos componente do android, bloqueamos esse tipo de interação.

```
<activity android:name=".SensiveActivity" android:exported="
   false" >
```

```
// Permissões
<permission android:name="com.example.myapp.MY_PERMISSION"
   android:protectionLevel="signature" />
```

```
// Verificação de intenção
Intent intent = getIntent()
Intent forward = (Intent) intent.getParcelableExtra("key");
ComponentName name = forward.resolveActivity(
   getPackageManager());
if (name.getPackageName().equals("safe_package") &&
        name.getClassName().equals("safe_class")) {
    startActivity(forward);
}

// Sanitização de intenção
Intent intent = new  IntentSanitizer.Builder()
 .allowComponent("com.example.ActivityA")
 .allowData("com.example")
 .allowType("text/plain")
 .build()
 .sanitizeByThrowing(intent);
```

Avaliação de conformidade

Além disso, foi feita a avaliação da força e garantia do modelo por meio da adequação à certificação PCI DSS com a verificação do cumprimento de 12 requisitos fundamentais exigidos pela organização.

PCI DSS

No quadro são mostrados os 12 requisitos exigidos pela certificação e marcados com "X" os quais o modelo proposto contempla.

Com base na análise por meio do PCI DSS chegamos aos seguintes pontos:

- Lacunas
- Especificidade
- Eficiência

Principais Requisitos do PCI DSS	Modelo
Instalar e manter controles de segurança de rede	X
Aplicar as configurações de segurança para todos os componentes de sistema	X
Proteger os dados da conta armazenados	X
Proteger os dados do titular do cartão com criptografia forte durante a transmissão em redes públicas abertas	X
Proteger todos os sistemas e redes de software malicioso	X
Desenvolver e manter sistemas e software seguros	X
Restringir o acesso aos componentes de sistema e aos dados do titular do cartão por necessidade de conhecimento do negócio	X
Identificar usuários e autenticar o acesso aos componentes de sistema	X
Restringir o acesso físico aos dados do titular do cartão	
Registrar e monitorar todo o acesso aos componentes de sistema e dados do titular do cartão	
Testar a segurança de sistemas e redes regularmente	
Apoiar a segurança com políticas e programas organizacionais	

Análises do trabalho

O resultado obtido neste estudo, isso é, o modelo de requisitos de segurança; está em consonância com as melhores práticas e recomendações encontradas na literatura sobre segurança em aplicações móveis, especialmente no contexto bancário.

Contribuições centrais

- Integração e modelagem de práticas recomendadas
- Referência para futuras aplicações
- Impactos positivos na segurança, confiança e conformidade

Limitações

- Avaliação em ambiente controlado
- Necessidade de atualizações contínuas
- Escopo focado nas principais ameaças

Conclusão

Conclusão

O trabalho proporciona uma base sólida e confiável para o desenvolvimento de aplicações bancárias seguras no Android, abordando as necessidades fundamentais de segurança no cenário de ameaças cibernéticas em constante evolução.

- **Caminhos da pesquisa**
- **Dificuldades encontradas**
- **Futuro da pesquisa**

Obrigado!!