Análise de Vulnerabilidades no Sistema NFC: Simulação de Interceptação e Mitigação Baseada em Software

Luiz Felipe Batista da Silva[1], José Antonio Silva de Araujo[1], Rick Dayvid da Costa Ferreira[1], Gilberto Gercino da Silva[1], Fábio Augusto Procópio de Paiva[1], Diego da Silva Pereira[1]

[1]Laboratório de Pesquisa em Redes e Sistemas Computacionais (NOCS LAB), Instituto Federal do Rio Grande do Norte, Parnamirim, Brasil (batista.felipe2@escolar.ifrn.edu.br)

Resumo: Este artigo visa analisar as vulnerabilidades do sistema NFC, com foco em ataques de Eavesdropping e Relay. Por meio de simulações com um leitor RFID no Wokwi e da análise do tráfego de rede via Wireshark, demonstrou-se a fragilidade da transmissão de dados em texto claro. Para mitigar essas falhas, propõe-se uma arquitetura de defesa no servidor desenvolvida em Java com Spring Boot, implementando tokens dinâmicos para garantir a integridade das transações.

Palavras-chave: NFC; Vulnerabilidades; Eavesdropping; Segurança de Redes; Spring Boot.

INTRODUÇÃO

Os avanços tecnológicos se intensificaram no decorrer do tempo, os serviços financeiros e os sistemas de comunicação adotam mais medidas para facilitar o dia a dia das pessoas. Entre as novas tecnologias, surgiu o NFC (Near Field Communication), que é um sistema sem fio de baixo alcance que permite o envio de informações entre dispositivos compatíveis com uma pequena aproximação entre eles.

O NFC foi desenvolvido a partir do sistema RFID (Radio Frequency Identification). Com isso, o NFC tem funcionalidades de comunicação por radiofrequência. Porém, os 2 sistemas possuem diferenças, como o NFC foi criado para funcionar com pequenas aproximações entre dispositivos.

O NFC funciona com uma frequência de 13,56 MHz (megahertz) e possui um baixo alcance, cerca de 4 centímetros. Essa tecnologia é bastante utilizada em pagamentos digitais, como em cartões bancários e sistemas de transporte, como em ônibus. Essa tecnologia se tornou muito popular devido aos pagamentos por aproximação feitos por celulares e cartões bancários.

A tecnologia apresenta funções de segurança como autenticação, criptografia e tokenização, visando garantir a integridade e a confidencialidade das informações transmitidas (LRI Automação Industrial, 2023; Costa, 2024). No entanto, algumas pesquisas internacionais mostram que o sistema NFC possui vulnerabilidades que podem comprometer a confidencialidade e a integridade das informações transmitidas. Entre os principais riscos, se destacam os ataques de interceptação (Eavesdropping), ataques de retransmissão (Relay Attack), exploração de brechas no sistema por meio de engenharia social e clonagem de etiquetas NFC.

Apesar de suas funcionalidades de segurança, o NFC demonstra ter vulnerabilidades que podem ser exploradas, entre eles, os ataques de interceptação (Eavesdropping), que capturam as informações transmitidas entre os dispositivos, os ataques de retransmissão (Relay Attack), que retransmite informações usando dispositivos intermediários, tendo em vista que o sistema possui baixo alcance, e a clonagem de etiquetas NFC, que permite a reprodução de informações em etiquetas compatíveis, são alguns dos exemplos que demonstram as vulnerabilidades do sistema.

Este trabalho tem como seus principais objetivos, analisar as vulnerabilidades de clonagem e interceptação do sistema NFC e propor uma arquitetura de defesa resiliente baseada em tokens dinâmicos desenvolvida em Java com Spring Boot.

MATERIAL E MÉTODOS

A metodologia desta pesquisa caracteriza-se como exploratória e aplicada, estruturada em duas frentes de análise: a percepção dos usuários e a simulação técnica de vulnerabilidades e defesas da tecnologia NFC.

Na primeira frente, de abordagem quantitativa, foi aplicado um questionário estruturado por meio da

plataforma Google Forms a uma amostra de 40 participantes, selecionados por amostragem de conveniência. O instrumento foi elaborado para coletar dados comportamentais, buscando identificar o nível de conhecimento dos usuários sobre a tecnologia NFC, a frequência de uso no cotidiano e a percepção de segurança nas transações por aproximação. A coleta ocorreu de forma voluntária e anônima, estabelecendo o panorama do fator humano para justificar a mitigação técnica de riscos.

Na frente técnica, adotou-se uma abordagem laboratorial simulada, dividida em três camadas de infraestrutura. Para demonstrar a vulnerabilidade na camada física, realizou-se uma simulação no ambiente virtual de IoT *Wokwi*, emulando um microcontrolador Arduino Uno acoplado a um módulo leitor RFID (modelo RC522). O objetivo foi atestar a viabilidade da captura passiva do Identificador Único (UID) de uma etiqueta operando na frequência de 13,56 MHz durante a leitura, caracterizando o vetor de clonagem.

Para a análise da camada de rede, simulou-se a retransmissão do dado capturado via linha de comando, utilizando a ferramenta nativa *cURL* para emular um cliente malicioso disparando requisições HTTP locais contendo cargas úteis (*payloads*) em formato JSON. Simultaneamente, o analisador de protocolos *Wireshark* foi configurado para monitorar a interface de rede virtual (*loopback*), com o intuito de inspecionar o tráfego e avaliar a legibilidade dos dados transacionais diante da ausência de protocolos de criptografia na comunicação.

Por fim, na camada de aplicação, desenvolveu-se uma API RESTful utilizando a linguagem Java (versão 17), o *framework Spring Boot* e gerenciamento de dependências via Maven. O sistema atuou como um servidor de autorização programado para mitigar as falhas emuladas, rejeitando requisições baseadas exclusivamente em UIDs estáticos e exigindo a validação de tokens criptográficos dinâmicos. Complementarmente, acoplou-se o banco de dados em memória H2 para o registro estruturado das tentativas de intrusão barradas pela rede.

RESULTADOS E DISCUSSÃO

Inicialmente, analisou-se a percepção dos usuários quanto à adoção cotidiana e à segurança da tecnologia NFC. Os dados coletados por meio do questionário revelaram um comportamento definido nesta pesquisa como o "Paradoxo da Conveniência". Considerando o recorte demográfico da amostra, composta majoritariamente por estudantes nativos digitais (97,5% concentrados na faixa etária entre 14 e 25 anos), observou-se uma alta taxa de usabilidade: 70% dos respondentes afirmam utilizar pagamentos por aproximação frequentemente em estabelecimentos comerciais, com destaque para supermercados (75%), shoppings (46,9%) e farmácias (37,5%)

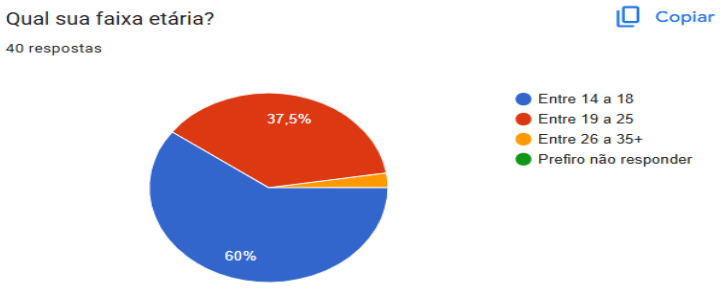

Figura 1. Faixa Etária.

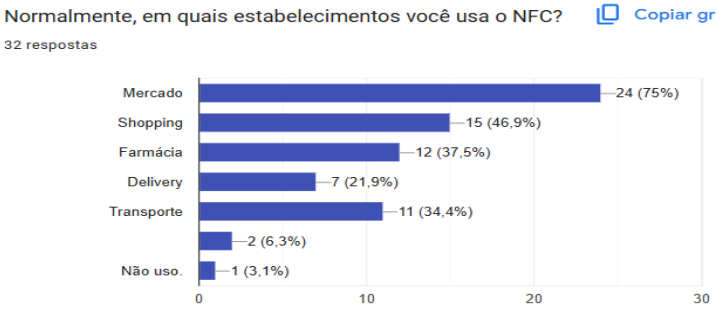

Figura 2. Principais estabelecimentos de uso.

Contudo, quando questionados sobre a confiabilidade do sistema, a maioria demonstrou ceticismo ou desinformação. Constatou-se que 57,5% dos usuários não consideram o meio de pagamento seguro e 20% admitem não compreender o funcionamento técnico da tecnologia. Ademais, 32,5% dos participantes afirmaram desconhecer totalmente os vetores de risco associados à aproximação, ao passo que 47,5% temem especificamente a clonagem de dados. Nota-se ainda uma distorção técnica quanto ao hardware: os respondentes tendem a atribuir maior segurança aos ecossistemas Android (47,4%) e Apple/iPhone (47,4%) em detrimento dos cartões físicos (31,6%)

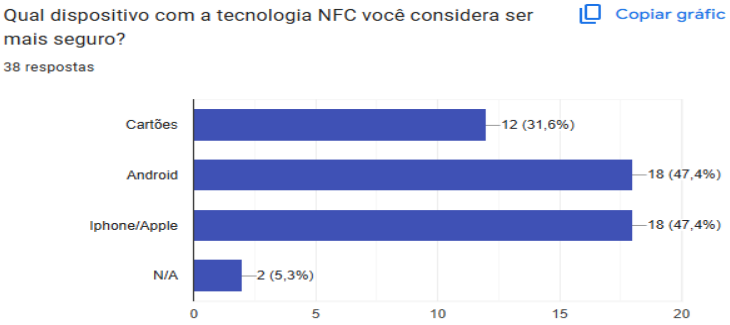

Figura 3: Dispositivos considerados seguros.

Sob a ótica da Engenharia de Sistemas, a intuição dos respondentes em atribuir maior confiabilidade aos smartphones em detrimento dos cartões físicos mostra-se acertada. De fato, o cartão plástico representa o elo mais vulnerável do ecossistema por operar sem verificação de portador (CVM). Para atestar essa fragilidade física, emulou-se um leitor RFID RC522 no ambiente *Wokwi* efetuando a leitura de uma etiqueta padrão. Comprovou-se que o hardware transmite o Identificador Único estático de forma passiva e em texto claro (UID: 04 11 22 33), viabilizando a clonagem imediata por dispositivos próximos, o que comprova a viabilidade de vetores de ataque periféricos (MDPI Sensors, 2024).

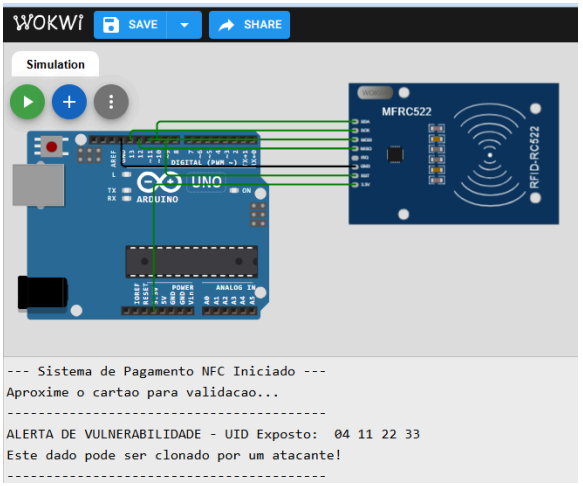

Figura 4: Captura passiva de UID em texto claro emulada no ambiente Wokwi.

Contudo, a premissa de que carteiras digitais proprietárias são estruturalmente invioláveis revela-se precipitada. Precedentes técnicos desmentem essa intuição absoluta: Radu et al. (2022) demonstraram que falhas lógicas na integração entre a rede Visa e o *Apple Pay* (operando no Modo Transporte Expresso) permitiram que invasores realizassem ataques de retransmissão (*Relay Attacks*) para aprovar transações de alto valor com o smartphone fisicamente bloqueado no bolso da vítima.

Na camada de transporte, a simulação de tráfego local inspecionada via *Wireshark* confirmou o sucesso de ataques de interceptação (*Eavesdropping*). Na ausência de encapsulamento criptográfico (como protocolos TLS/HTTPS), pacotes HTTP contendo dados transacionais e identificadores de cartões trafegam totalmente expostos na rede, permitindo a captura de cargas úteis (*payloads*) por intermediários maliciosos.

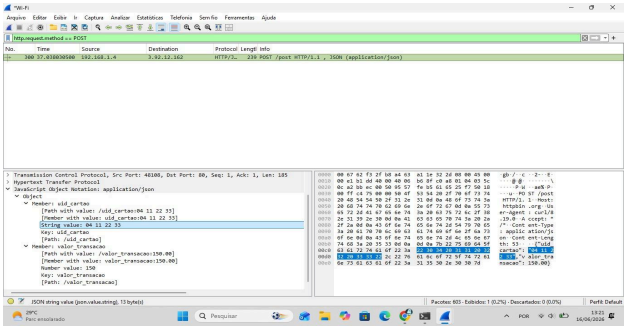

Figura 5: Interceptação de pacotes via Wireshark expondo parâmetros transacionais.

A superação definitiva dessas vulnerabilidades exige a aplicação do princípio de Desconfiança Zero (*Zero Trust*) no servidor (*back-end*), modelo arquitetural introduzido por Kindervag (2010) e formalmente padronizado pelo *National Institute of Standards and Technology* (NIST, 2020) sob a premissa de que nenhum vetor — interno ou periférico — é plenamente confiável por padrão. Precedentes na literatura ratificam essa necessidade: Radu et al. (2022) demonstraram que a ausência de checagens rigorosas no servidor permitiu que invasores realizassem ataques de retransmissão (Relay Attacks) no Apple Pay (rede Visa) em smartphones bloqueados no Modo Transporte Expresso.

Em nossa arquitetura desenvolvida em Spring Boot, a validação não confia no dispositivo periférico; a aprovação exige um token criptográfico dinâmico gerado em tempo de execução. Ao receber uma requisição maliciosa contendo apenas o UID clonado (04 11 22 33), a API rejeita a transação e retorna o código HTTP 401 Unauthorized, registrando a tentativa de intrusão com carimbo de tempo (timestamp), inviabilizando ataques de retransmissão estática (Stripe, 2024; Spring Framework, 2026).

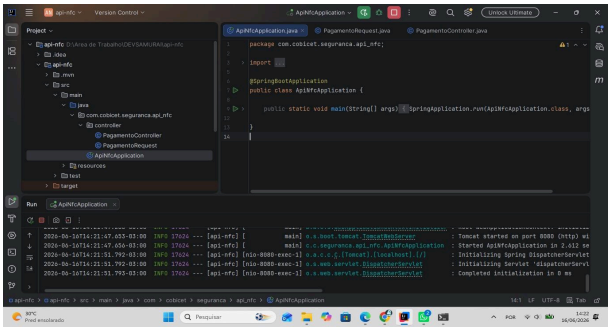

Figura 6: Estrutura do servidor de autorização.

Figura 7: Bloqueio de ataque de clonagem retornado pela barreira de segurança no Spring Boot.

CONCLUSÃO

Conclui-se, portanto, que a tecnologia NFC, embora seja amplamente consolidada pela conveniência comercial, apresenta vulnerabilidades estruturais críticas em suas camadas física e de transporte quando operada sem salvaguardas de software. A Prova de Conceito demonstrou que a passividade do hardware periférico permite a clonagem de UIDs e ataques de interceptação em redes locais. Contudo, atestou-se a eficácia da transferência da responsabilidade de segurança para a camada de aplicação: a implementação de uma API RESTful baseada em Spring Boot validou a capacidade de neutralizar retransmissões maliciosas por meio da exigência de tokens dinâmicos, alinhando a percepção de segurança dos usuários à resiliência técnica do sistema.

AGRADECIMENTOS

Agradecemos ao Professor Diego da Silva Pereira do NOCS LAB, pela orientação e pela oportunidade de desenvolver esse trabalho.

REFERÊNCIAS

RADU, A.-I. et al. Practical EMV Relay Protection. *IEEE Symposium on Security and Privacy (S&P)*, San Francisco, p. 1737-1756, 2022. Disponível em: https://practical_emv.gitl.ab.io/assets/practical_emv_rp.pdf . Acessado em: 22 maio 2026.

Costa, M. W. O. A Segurança por trás da Tecnologia NFC. *Trabalho de Conclusão de Curso (Tecnologia em Redes de Computadores)* – Faculdade Estácio, 2024. Disponível em: https://pt.slideshare.net/slideshow/artigo-marcus-winicius-oliveira-costa-a-segurana-por-trs-da-tecnologia-nfc/266708076. Acessado em: 05 jun. 2026.

ePrint Archive. Relay Attack. Disponível em: https://eprint.iacr.org/2010/228. Acessado em: 27 maio 2026.

KINDERVAG, J. Build Security Into Your Network's Genesis: The Zero Trust Network Architecture. *Forrester Research*, Cambridge, p. 1-14, 2010.

LRI Automação Industrial. Segurança em NFC: Entenda os Recursos e Práticas de Proteção. *Blog LRI*, 2023. Disponível em: https://blog.lri.com.br/seguranca-em-nfc/. Acessado em: 22 maio 2026.

MDPI Sensors. Advances in Near Field Communication Security and Eavesdropping Mitigation. *Sensors Journal*, v. 24, n. 23, p. 7423, 2024. Disponível em: https://www.mdpi.com/1424-8220/24/23/7423. Acessado em: 22 maio 2026.

NFC Forum. What NFC Does. Disponível em: https://nfc-forum.org/learn/what-nfc-does/. Acessado em: 04 jun. 2026.

NIST. Zero Trust Architecture. *National Institute of Standards and Technology*, Special Publication 800-207, Gaithersburg, 2020. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-207/final. Acessado em: 20 jun. 2026.

Spring Framework. Spring Boot Reference Documentation. *Spring Docs*, 2026. Disponível em: https://docs.spring.io/spring-boot/. Acessado em: 16 jun. 2026.

Stripe. NFC Security 101: A Guide for Businesses Using Contactless Payments. *Stripe Resources*, 2024. Disponível em: https://stripe.com/br/resources/more/nfc-security-101-a-guide-for-businesses-using-contactless-payments. Acessado em: 10 jun. 2026.