INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS FLORIANO
CURSO TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

IANDER MIRANDA FERNANDES

SEGURANÇA DE DADOS: Análise sobre técnicas de autenticação em redes

FLORIANO

2025

IANDER MIRANDA FERNANDES

SEGURANÇA DE DADOS: Análise sobre técnicas de autenticação em redes

Trabalho de Conclusão de Curso (artigo científico) apresentado como exigência parcial para obtenção do diploma do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Floriano .

Orientador: Prof. Me. Marcony Santana Máximo

FLORIANO

2024

SEGURANÇA DE DADOS: Análise sobre técnicas de autenticação em redes

Iander Miranda Fernandes[1]
Prof. Me. Marcony Santana Máximo[2]

RESUMO

Este estudo consiste em uma pesquisa de revisão da literatura de caráter qualiquantitativo focalizada na segurança de dados, com ênfase nas técnicas de autenticação e teve como objetivo geral investigar e compreender as técnicas de autenticação empregadas na segurança de dados, abordando suas aplicações, benefícios e desafios. Para alcançar esse objetivo, foram definidos os seguintes objetivos específicos: investigar e compreender as técnicas de autenticação como uma camada essencial na segurança de dados, analisar os diferentes métodos de autenticação existentes e avaliar as vantagens e desvantagens de cada método de autenticação em termos de segurança e usabilidade. Com o objetivo de alcançar os resultados previstos inicialmente, foram utilizadas bases de dados como IEEE e Scopus, foi implementada uma estratégia de busca com palavras-chave relacionadas, como "segurança de dados" e "métodos de autenticação", em conjunto com termos específicos para os métodos selecionados. Em seguida, uma leitura completa dos artigos selecionados foi realizada para extrair informações pertinentes. Posteriormente, uma análise comparativa dos métodos de autenticação destacados no estudo foi conduzida, observando características distintivas, recomendações de aplicação, níveis de segurança e eficácia de cada método. Os principais dados identificados foram discutidos com base nos objetivos da pesquisa
Palavras-chave: Segurança de dados; Autenticação; Métodos de autenticação; Biometria.

ABSTRACT

This study consisted of a literature review focused on data security, with an emphasis on authentication techniques. Using databases such as IEEE and Scopus, a search strategy was implemented with related keywords, such as "data security" and "authentication methods", together with specific terms for the selected methods. The inclusion and exclusion criteria established the selection of studies published in the last 10 years, in English or Portuguese, and specifically related to the topic. The initial screening of studies was based on these criteria, analyzing titles and abstracts to identify the most relevant studies. Then, a complete reading of the selected articles was carried out to extract pertinent information. Subsequently, a comparative analysis of the authentication methods highlighted in the study was conducted, observing distinctive characteristics, application recommendations, security levels and effectiveness of each method. The main data identified were discussed based on the research objectives.

Keywords: Data security; Authentication; Authentication methods; Biometry.

Data de aprovação: 04/07/2024

---

[1] Graduando em Tecnologia em Análise e Desenvolvimento de Sistemas. Instituto Federal do Piauí. iander.fmiranda@gmail.com .
[2] Professor Mestre em Propriedade Intelectual. Instituto Federal do Piauí. marconysantanamaximo@gmail.com .

1 INTRODUÇÃO

A segurança de dados em meios digitais é um assunto de extrema importância na sociedade, refere-se a um conjunto de medidas, práticas e tecnológicas empregadas para garantir a confidencialidade, integridade e disponibilidade de dados. Conforme a norma da ABNT (2005), a segurança da informação corresponde à proteção de informações quanto a vários tipos de ameaças, visando garantir a continuidade e minimização aos riscos do negócio, além de maximizar o retorno sobre os investimentos e as oportunidades do negócio.

Segundo o relatório publicado, a Fortinet, uma das maiores empresas especializadas em segurança cibernética, através do seu laboratório de inteligência de ameaças FortiGuard Labs, informou que houve mais de 41 bilhões de tentativas de ataque cibernético em 2020 em toda a América Latina e Caribe. Sendo que 8,4 bilhões dessas tentativas foram destinadas ao Brasil. Ameaças conhecidas (malware, por exemplo), foram detectadas. Foi observado também a eficiência que os cibercriminosos estão alcançando ao utilizarem tecnologias avançadas e Inteligência Artificial (IA) para que o ataque seja mais direcionado e realizado em menos tentativas. (Fortinet, 2021).

Com a rápida evolução da tecnologia e a crescente dependência de sistemas de informações, proteger os dados contra ameaças cibernéticas tornou-se uma preocupação primordial para indivíduos, empresas e organizações em todo o mundo. Lyra (2008) enfatiza que a segurança da informação é obtida mediante a implementação de um conjunto de controles adequados que inclui políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Controlar o acesso a sistemas computacionais torna-se cada vez mais importante na contemporaneidade, e o mecanismo mais conhecido e usual para garantir a segurança em sistemas de informação é através da autenticação (Costa et al., 2005).

A autenticação é uma das diversas técnicas de segurança de dados que existem. Segundo Silva et al. (2019), é um recurso para proteger informações em um sistema onde é comum utilizar senhas ou cartões magnéticos. Não obstante, dentre os métodos de autenticação tradicionais existentes pode citar-se: Senhas, é o método de autenticação mais comum, em que os usuários inserem uma combinação

de caracteres (senha) para verificar sua identidade. Tokens de autenticação, envolve o uso de dispositivos físicos (tokens) que geram códigos únicos e temporários que são inseridos junto com a senha para autenticar o usuário. Biometria, utiliza-se características físicas ou comportamentais exclusivas, como impressões digitais, reconhecimento facial, íris, voz ou assinatura, para verificar a identidade de um indivíduo. Cartões inteligentes, envolve o uso de cartões físicos contendo informações criptografadas e chaves de autenticação que são inseridos em leitores para autenticar o usuário. Certificados digitais, baseados em criptografia de chave pública, os certificados digitais são emitidos por autoridades de certificação confiáveis e oferecem uma forma de autenticação e verificação de identidade online.

A partir desse contexto, esse trabalho tem como objetivo principal, analisar os métodos tradicionais de autenticação, compreendidos nesta pesquisa, verificar suas vantagens, desvantagens e vulnerabilidades. Guiado pela seguinte questão: Quais as características, vantagens e desvantagens dos métodos tradicionais de autenticação, baseado em segurança e usabilidade?

No que tange aos objetivos específicos pretende investigar e compreender as técnicas de autenticação como uma camada essencial na segurança de dados, analisar os diferentes métodos de autenticação existentes, avaliar as vantagens e desvantagens de cada método de autenticação em termos de segurança e usabilidade.

2 REFERENCIAL TEÓRICO

A segurança digital depende da segurança de dados, e usá-los em redes é fundamental para garantir a integridade, confidencialidade e disponibilidade da informação. A proteção de dados nas redes modernas é mais do que uma mera precaução; é a garantia de uma sociedade digital robusta, onde a segurança e a privacidade coexistem. Na perspectiva de Sousa (2010) o uso de tecnologias de comunicação sem fio entre dispositivos aumentou a mobilidade e a comodidade dos usuários. A IEEE 802.11 [IEEE Standard 802.11 1999], mais comumente conhecida como Wi-Fi, é a norma principal de rede sem fio usada atualmente tanto para estabelecer redes locais quanto para acessar a Internet

A aplicação eficaz das definições básicas de segurança de dados em redes é a chave para mitigar ameaças cibernéticas, garantindo que as informações críticas

permaneçam protegidas contra qualquer tentativa de acesso não autorizado. A segurança de dados em redes é uma necessidade em um mundo conectado. A preservação da confiança digital depende da compreensão e melhoria das medidas de segurança. Sousa (2010, p. 3) aponta:

> Apesar dos objetivos de garantia de segurança aos clientes da rede, os protocolos de proteção às redes IEEE 802.11 ainda apresentam significativas vulnerabilidades. Os problemas, em geral, são derivados do meio não guiado e sem controle por onde trafegam as informações. Este tipo de propagação de informações se mostra inerentemente inseguro, visto que os dados podem ser capturados por dispositivos maliciosos.

No cenário da segurança em redes, Nakamura e Geus (2002) apontam que seja frente à violências urbanas ou na defesa contra invasores externos, destaca-se a importância dessa peculiar forma de prevenção a ataques. Nesse contexto, destaca-se uma evolução contínua, em que a cada novo ataque a criação de contramedidas inovadoras é indispensável. Essas contramedidas, por sua vez, estimulam o desenvolvimento de novas estratégias e métodos ofensivos, formando assim um ciclo de adaptação constante.

A autenticação é um pilar fundamental da segurança cibernética, garantindo que apenas usuários autorizados tenham acesso aos sistemas e recursos. Tradicionalmente, a autenticação é realizada por meio de algo que o usuário sabe, como senhas, algo que o usuário possui, como chaves de segurança físicas, ou algo que o usuário é, como reconhecimento biométrico. No entanto, de acordo com Nakamura e Geus (2002) com o aumento das ameaças cibernéticas, as abordagens de autenticação estão evoluindo para incluir métodos mais robustos e multifatoriais, a autenticação de dois fatores, por exemplo, combina duas formas de verificação de identidade para fortalecer a segurança. Além disso, tecnologias emergentes, como a autenticação baseada em comportamento e a análise de contexto, estão sendo exploradas para melhorar a detecção de atividades suspeitas e proteger contra ataques sofisticados.

Em um cenário em constante evolução, a autenticação continua sendo um aspecto crucial da defesa cibernética, exigindo uma abordagem adaptativa e em camadas para garantir a segurança dos sistemas e dados sensíveis. As técnicas de autenticação em redes são uma parte importante das várias estratégias inovadoras para melhorar a segurança de dados. O processo de verificação da identidade de um usuário, dispositivo ou sistema para garantir que apenas os usuários autorizados possam usar os recursos desejados é conhecido como autenticação.

Thian (2001) segundo Magalhães (2003) aponta que a autenticação e a identificação são as duas categorias de problemas relacionados à criação de uma associação entre uma pessoa e uma identidade. A identificação envolve estabelecer uma identidade de uma pessoa desconhecida à partida, enquanto uma identidade envolve confirmar ou negar uma alegada de uma pessoa.

Cada uma das várias técnicas de autenticação é usada para proteger as redes. Embora uma autenticação baseada em informações pessoais do usuário, como senhas, seja comum, ela pode ser ineficaz por ataques de força bruta. Assim, métodos adicionais, como autenticação de dois fatores (2FA) ou autenticação multifatorial (MFA), que ativam a apresentação de duas ou mais formas de identificação, têm ganhado popularidade.

Tradicionalmente, a busca por um método de autenticação inclui sistemas que envolvem a transferência de segredos entre o usuário e o objeto de segurança. O segredo, como todos os segredos, pode ser cedido voluntariamente a terceiros por quem o conhece, ou que o torna transmissível. A necessidade de armazenamento ou memorização de segredos é outro problema com este método Magalhães (2003).

O alto índice de pesquisas por métodos de autenticação tem sido extensa e normalmente inclui sistemas secretos com o dispositivo de segurança e o usuário. Mas este método tem alguns problemas. A transmissibilidade de segredos, que pode ser compartilhada voluntariamente ou involuntariamente por quem o conhece, constitui um problema significativo e pode representar um risco à segurança. Além disso, manter segredos é difícil. As deficiências intrínsecas dos sistemas de armazenamento são herdadas quando o segredo é armazenado. Por outro lado, a memorização é propensa ao esquecimento, o que muitas vezes leva a usar segredos simples para facilitar a memorização. Esses problemas enfatizam a necessidade de métodos de autenticação mais sofisticados e seguros que superem as limitações.

Linhares (2007) destaca o avanço de sistemas de segurança em redes de alta qualidade tipicamente fundamenta-se em três premissas essenciais: confiança, autenticação e integridade.

A biometria é uma tecnologia que verifica a identidade de uma pessoa usando características físicas ou comportamentais exclusivas, como fluxo digital, brilho e reconhecimento facial e vocal (Costa et al. 2022, p. 104). As características biométricas são intrinsecamente ligadas à pessoa, poucas variações na

probabilidade de falsificação. A autenticação biométrica é amplamente utilizada em sistemas de segurança, controle de acesso e dispositivos eletrônicos, oferecendo uma abordagem avançada para proteger as informações e garantir que a identidade do usuário seja realmente conhecida.

Atualmente, várias características são usadas separadamente ou em conjunto para autenticar e/ou identificar uma pessoa. Como observado por Souza e Gonçalves (2010), uma variedade de fatores pode ser usada para avaliar cada método. Esses fatores incluem confiabilidade, nível de conforto, facilidade por parte dos usuários e custos de implementação.

A biometria elimina a necessidade de memorização ou posse de objetos físicos, tornando uma experiência mais fácil e intuitiva. Isso é a diferença dos métodos tradicionais, como senhas ou cartões. Essa abordagem possui uma variedade de aplicativos, incluindo desbloqueio de smartphones, controle de fronteiras e a segurança da indústria, promovendo uma autenticação mais eficaz

> Ao longo dos anos a investigação científica tem-se dedicado também ao estudo de biometrias que não avaliam características físicas, mas sim comportamentais, como a forma como um utilizador digita os caracteres num teclado, a forma como um cidadão caminha num corredor ou a força com que aperta o manípulo de uma porta ao abri-la (Magalhães, 2003, p. 2).

A escolha do(s) método(s) a utilizar depende da análise de risco que necessariamente deve ser feita, relativamente à informação/infraestrutura que se pretende proteger. Por exemplo, o aeroporto Narita (Tóquio) pretende implementar um processo de autenticação que inclui o reconhecimento de rosto e o reconhecimento da íris em conjunção. A Central Intelligence Agency (CIA), o Federal Bureau of Investigation (FBI) e a National Aeronautics and Space Administration (NASA) utilizam leitores de retina para proteger o acesso a zonas sensíveis. No entanto, seria excessivamente dispendioso e desajustado utilizar leitores de retina ou de íris para autenticar/identificar o utilizador de um computador pessoal no laboratório de informática de uma universidade Magalhães (2003).

A biometria se mostra um método de autenticação consideravelmente seguro de acordo com as condições em que são aplicadas. O exemplo dado acima de acordo com Magalhães (2003) é uma visão prática deste exemplo. Diversos métodos de autenticação são empregados para verificar a identidade de usuários em sistemas digitais, sendo a escolha do método influenciada pelo nível de

segurança requerido e pelas características particulares do sistema em questão. Em ambientes digitais, existem vários métodos para confirmar a identidade dos usuários.

São empregadas autenticações de uso frequente como exemplo as senhas que oferecem familiaridade, simplicidade e simples de implementar. Porém até este método mais simples tem desafios substanciais, como ataques de força bruta e phishing. A autenticação de Dois Fatores (2FA) ou multifatorial é uma estratégia que fortalece a segurança, requerendo, além da senha, um segundo fator como código gerado, token ou aplicativo de autenticação. Embora forneça uma camada extra de proteção, pode ser percebida como menos conveniente para alguns usuários, exigindo a gestão de dispositivos ou códigos adicionais.

Os certificados digitais são uma alternativa que utiliza chaves criptográficas para autenticar usuários e garantir a integridade das comunicações. Apesar de proporcionarem uma segurança sólida, a implementação e gestão desses certificados podem ser complexas, exigindo uma infraestrutura de chave pública.

Os cartões inteligentes, como os Smart Cards, são dispositivos físicos que armazenam informações de autenticação. Essa abordagem fornece uma solução 9 tangível e difícil de replicar, mas está sujeita a riscos de perdas ou roubos, além de implicar custos associados à implementação. Esse pensamento se desenvolve a partir de Lorenzoni (2006, p. 14) que afirma:

> Nota-se, desde sua invenção em 1974, uma grande evolução na área dos cartões inteligentes, tanto da parte física e suas funcionalidades quanto dos ambientes de desenvolvimento e tecnologias usadas para sua programação. Devido às suas características, muitas aplicações utilizam e utilizarão essa tecnologia, tais como: sistemas de identificação, sistemas de transações bancárias, certificação digital entre outras tantas. A tendência mundial para os próximos anos, é o crescimento das mais variadas aplicações com o uso dos smart cards.

Cada método de autenticação apresenta suas vantagens e desvantagens, sendo imperativo considerar a aplicação específica e os requisitos de segurança ao escolher a abordagem mais adequada para um sistema específico como é abordado e evidenciado na tabela 1, onde é listado os métodos, vantagens, desvantagens e características.

Tabela 1 – Métodos de autenticação

Método de Autenticação	**Vantagens**	**Desvantagens**	**Caracteristicas**
Senha	Fácil de implementar e usar	Vulnerável a ataques de força bruta e phishing	Requer políticas de senha forte e trocas regulares
	Baixo custo	Pode ser esquecida ou comprometida facilmente	Bloqueio após várias tentativas de login malsucedidas
Autenticação de dois fatores (2FA) e MFA	Adiciona uma camada extra de segurança	Pode ser mais inconveniente para os usuários	Fornece um segundo fator de verificação
	Reduz o risco de acesso não autorizado	Dependência de dispositivos adicionais pode ser custosa	Métodos incluem SMS, aplicativos de autenticação, etc.
	Dificulta a ação de invasores mesmo se a senha for roubada	Requer configuração adicional na infraestrutura	Pode utilizar tokens físicos ou virtuais
	Altamente segura e difícil de falsificar	Requer infra estrutura de PKI (Public Key Infrastructure)	Usa certificados digitais únicos para cada entidade
Autenticação baseada em Certificados Digitais	Elimina a necessidade de senhas	Complexa de implementar e gerenciar	Comunicações são criptografadas usando certificados
			Certificados precisam ser emitidos e

			revogados corretamente
Autenticação Biométrica	Muito segura, baseada em características únicas do usuário	Pode ser cara e complexa de implementar	Pode usar impressão digital, reconhecimento facial, etc.
	Elimina a necessidade de senhas	Pode haver problemas de privacidade e aceitação do usuário	Exige hardware e software especializado
	Gera códigos únicos que mudam regularmente	Possibilidade de perda ou roubo do token	Reduz o risco de acesso não autorizado mesmo se a senha for roubada
Autenticação por Token	Alta segurança	Custos associados à emissão e distribuição de tokens	Pode ser físico ou baseado em aplicativos
			Necessidade de sincronização entre o token e o servidor de autenticação

Fonte: Autoria própria (2024).

3 CONSIDERAÇÕES FINAIS

A evolução rápida da tecnologia e a dependência cada vez maior de sistemas de informação ressaltam a importância crucial de proteger dados contra ameaças cibernéticas. Nesse contexto, a autenticação emerge como um componente vital na implementação de

medidas de segurança. A autenticação, seja por senhas, tokens, biometria, cartões inteligentes ou certificados digitais, é fundamental para controlar o acesso a sistemas computacionais.

No âmbito dos objetivos gerais, a pesquisa buscou fornecer uma compreensão abrangente das técnicas de autenticação utilizadas na segurança de dados, avaliando suas aplicações práticas, benefícios e desafios associados. Dessa forma, a análise proposta contribui para o aprimoramento contínuo das práticas de segurança cibernética, visando garantir a confidencialidade, integridade e disponibilidade dos dados em um ambiente digital cada vez mais complexo e vulnerável a ameaças.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799: Tecnologia da informação, técnicas de segurança - código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2005. Disponível em: https://tororodeideias.files.wordpress.com/2012/03/nbr-iso-iec-17799.pdf. Acesso em: 20 jun. 2024.

COSTA, Carlos et al. **Autenticação biométrica via dinâmica da digitação em teclados numéricos.** *In*: SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES, 22., 2005, São Paulo. **Anais** […]. São Paulo, 2005. Disponível em: https://www.decom.fee.unicamp.br/lpdf/publicacoes_pdf/Carlos_SBrT05.pdf. Acesso em: 18 maio 2024.

COSTA, Luciano R. et al. **Introdução à Biometria**. *In*: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 6., 2022, Santa Catarina. **Anais** […]. Santa Catarina, 2022. Disponível em: https://sol.sbc.org.br/livros/index.php/sbc/catalog/download/101/455/726-1. Acesso em: 15 maio 2024.

FORTINET. **A América Latina sofreu mais de 41 bilhões tentativas de ataques cibernéticos em 2020**. [S. l.]: Fortinet, 2021. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2021/latin-america-suffered-more-than-41-billion-cyberattack-attempts-in-2020. Acesso em: 17 abr. 2024.

LINHARES, André G. **Uma análise do mecanismo de segurança de redes IEEE 802.11: WEP**. 2007. Trabalho de Conclusão de Curso (Graduação) – Universidade Federal de Pernambuco, Recife, 2007.

LORENZONI, Álvaro F. **Smart cards: Java Cards**. 2006. Trabalho de Conclusão de Curso (Graduação) – Centro Universitário Feevale, Novo Hamburgo, 2006.

LYRA, Maurício R. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Ciência Moderna, 2008.

MAGALHÃES, Paulo S. **Biometria e autenticação**. *In*: CONFERÊNCIA DA ASSOCIAÇÃO PORTUGUESA DE SISTEMAS DE INFORMAÇÃO, 4., 2003, Porto. **Actas** […]. Porto, 2003. Acesso em: 15 dez. 2023.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. **Segurança de redes**. Berkeley: [s. n.], 2002.

SILVA, Rafael et al. **Autenticação biométrica para sistemas por meio da dinâmica da digitação.** Colloquium Exactarum, São Paulo, v. 11, n. 2, 2019. Disponível em: https://journal.unoeste.br/index.php/ce/article/view/3164/2793. Acesso em: 17 maio 2024.

SOUSA, Eduardo F. **Mecanismos de autenticação em redes IEEE 802.11**. 2010. Trabalho de Conclusão de Curso (Graduação) – Universidade Federal de Pernambuco, Recife, 2010.

SOUSA, Eduardo F.; GONÇALVES, P. A. S. **Segurança em Redes IEEE 802.11: Integridade de Dados, Autenticação e Confidência.** *In*: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 10., 2010. **Anais** […]. Pernambuco: Universidade Federal de Pernambuco, 2010. p. 119-131.