Autenticação Baseada em Tokens e Provas de Conhecimento Zero

Yasmin M. S. Criôlo[1], **Ruy J. G. B. de Queiroz**[1]

[1]Centro de Informática – Universidade Federal de Pernambuco (UFPE)
Caixa Postal 7851 – 50732-970 – Recife – PE – Brazil

ymsc@cin.ufpe.br, ruy@cin.ufpe.br

Abstract. *Authentication mechanisms are a fundamental component of modern digital systems. Token-based approaches are widely adopted due to their simplicity and scalability, but they present well-known security limitations. Zero-Knowledge Proofs emerge as an alternative paradigm that enables authentication without revealing secret information. This paper provides a conceptual, didactic and critical analysis that compares token-based authentication and zero-knowledge-based approaches, aiming to establish a theoretical foundation for further research.*

Resumo. *A autenticação constitui um dos pilares centrais da segurança em sistemas digitais contemporâneos. Entre os mecanismos mais utilizados, destacam-se os métodos de autenticação baseados em tokens, amplamente adotados devido à sua simplicidade, eficiência e facilidade de integração, mas que apresentam limitações de segurança recorrentes, como interceptação, reutilização indevida e dependência do canal de comunicação. Como alternativa conceitual, as Provas de Conhecimento Zero permitem a verificação de identidade sem a necessidade de revelar ou transmitir informações sensíveis. Este artigo apresenta uma análise conceitual, didática e comparativa entre a autenticação baseada em tokens e abordagens fundamentadas em Provas de Conhecimento Zero, discutindo seus princípios, vantagens, limitações e implicações para o desenvolvimento de mecanismos de autenticação mais seguros.*

1. Introdução

A autenticação é um componente fundamental da segurança da informação, sendo responsável por verificar a identidade de usuários e entidades em sistemas digitais [Menezes et al. 1996, Gollmann 2011].

Atualmente, grande parte das aplicações adota mecanismos de autenticação baseados em tokens, como senhas temporárias e JSON Web Tokens (JWT), devido à simplicidade, eficiência e facilidade de integração com aplicações web e serviços distribuídos [Jones et al. 2015].

Apesar de sua ampla adoção, mecanismos baseados em tokens apresentam vulnerabilidades recorrentes relacionadas ao roubo, interceptação e reutilização de credenciais, especialmente em ataques de repetição e phishing [Gollmann 2011].

Como alternativa criptográfica, as Provas de Conhecimento Zero (Zero-Knowledge Proofs – ZKP) permitem que uma entidade demonstre conhecimento de uma informação secreta sem revelar o próprio segredo [Goldwasser et al. 1989].

Nos últimos anos, construções modernas como zk-SNARKs e zk-STARKs ampliaram significativamente o interesse acadêmico e industrial em mecanismos de autenticação preservando privacidade e computação verificável.

Este trabalho apresenta uma análise conceitual e comparativa entre mecanismos de autenticação baseados em tokens e abordagens fundamentadas em ZKP, discutindo vantagens, limitações e desafios práticos dessas construções.

2. Autenticação Baseada em Tokens

2.1. Conceitos Básicos

A autenticação baseada em tokens consiste na utilização de um artefato digital que representa a identidade autenticada de um usuário ou entidade. Após um processo inicial de autenticação, o sistema emite um token que passa a ser utilizado como prova de identidade em interações subsequentes.

Entre os mecanismos mais comuns destacam-se senhas temporárias baseadas em tempo (Time-Based One-Time Passwords – TOTP) [M'Raihi et al. 2011] e JSON Web Tokens (JWT) [Jones et al. 2015].

A popularidade desses mecanismos decorre de vantagens práticas como facilidade de implementação, compatibilidade com diferentes plataformas e baixo custo computacional.

2.2. Limitações de Segurança

Como tokens precisam ser transmitidos e armazenados, eles podem ser interceptados, copiados ou reutilizados por atacantes em ataques de repetição.

Mesmo com mecanismos de expiração e proteção de canal, a dependência de um autenticador reutilizável representa um ponto crítico de vulnerabilidade, especialmente em cenários sujeitos a phishing e vazamento de credenciais.

3. Provas de Conhecimento Zero

3.1. Fundamentos

As Provas de Conhecimento Zero foram formalizadas por Goldwasser, Micali e Rackoff [Goldwasser et al. 1989] no contexto de sistemas de provas interativas. O objetivo dessas provas é permitir que um provador convença um verificador da validade de uma afirmação sem revelar qualquer informação adicional além da própria validade da afirmação.

Formalmente, provas de conhecimento zero devem satisfazer propriedades de completude, solidez (*soundness*) e conhecimento zero (*zero-knowledge*) [Goldwasser et al. 1989].

Posteriormente, Feige, Fiat e Shamir [Feige et al. 1988] exploraram aplicações dessas provas em protocolos de autenticação e identificação.

3.2. zk-SNARKs e zk-STARKs

Com o avanço das pesquisas surgiram construções modernas como zk-SNARKs, caracterizadas por provas curtas e verificação eficiente.

Protocolos como Pinocchio [Parno et al. 2013] e Groth16 [Groth 2016] estabeleceram bases importantes para aplicações práticas em computação verificável.

Mais recentemente, arquiteturas como Jolt [Arun et al. 2024] passaram a explorar modelos flexíveis para execução verificável de programas arbitrários.

Além das zk-SNARKs, construções como zk-STARKs vêm recebendo atenção crescente devido à ausência de *trusted setup* e potencial resistência pós-quântica [Ben-Sasson et al. 2018].

Apesar dessas vantagens, construções modernas de ZKP ainda apresentam custos computacionais significativamente superiores aos observados em mecanismos tradicionais de autenticação leve [Liang et al. 2025].

4. Comparação Conceitual

A principal diferença entre autenticação baseada em tokens e autenticação fundamentada em ZKP reside na natureza da informação utilizada durante o processo de autenticação.

Em mecanismos baseados em tokens, a autenticação depende da posse e apresentação de um artefato reutilizável previamente emitido pelo sistema. Em contraste, protocolos baseados em ZKP permitem demonstrar conhecimento de uma informação secreta sem revelar o segredo ou transmitir um autenticador reutilizável.

Essa distinção reduz riscos associados à reutilização indevida de credenciais, embora introduza desafios relacionados à eficiência computacional e complexidade de implementação.

Embora protocolos fundamentados em ZKP ofereçam vantagens relacionadas à privacidade, mecanismos baseados em tokens continuam mais eficientes e simples de implementar em aplicações convencionais.

Tabela 1. Comparação entre mecanismos de autenticação

Critério	**Tokens**	**zk-SNARKs**	**zk-STARKs**
Transmissão de segredo	Sim	Não	Não
Trusted setup	Não	Frequentemente necessário	Não
Tamanho da prova	Pequeno	Muito pequeno	Maior
Verificação	Rápida	Muito rápida	Rápida
Resistência pós-quântica	Limitada	Limitada	Potencialmente maior
Complexidade computacional	Baixa	Alta	Alta
Privacidade	Limitada	Elevada	Elevada

5. Conclusão

Este artigo apresentou uma análise conceitual entre mecanismos de autenticação baseados em tokens e abordagens fundamentadas em Provas de Conhecimento Zero.

A discussão evidenciou que, embora mecanismos tradicionais permaneçam amplamente utilizados devido à simplicidade e eficiência operacional, construções modernas de ZKP oferecem vantagens relevantes relacionadas à privacidade e redução da exposição de credenciais reutilizáveis.

Além disso, o avanço recente de construções como zk-SNARKs e zk-STARKs demonstra uma aproximação progressiva entre fundamentação criptográfica formal e aplicações práticas em sistemas distribuídos modernos.

Entretanto, desafios relacionados à eficiência computacional, escalabilidade e complexidade de implementação ainda representam obstáculos importantes para adoção ampla dessas construções em sistemas reais de autenticação.

Como continuidade deste trabalho, investigações futuras podem explorar avaliações experimentais de desempenho e modelos híbridos capazes de conciliar eficiência operacional e robustez criptográfica.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

Referências

Arun, A., Setty, S., Thaler, J., and Wahby, R. (2024). Jolt: Snarks for virtual machines via lookups. In *Advances in Cryptology – EUROCRYPT 2024*.

Ben-Sasson, E., Bentov, I., Horesh, Y., and Riabzev, M. (2018). Scalable, transparent, and post-quantum secure computational integrity. *IACR ePrint Archive*.

Feige, U., Fiat, A., and Shamir, A. (1988). Zero-knowledge proofs of identity. *Journal of Cryptology*, 1(2):77–94.

Goldwasser, S., Micali, S., and Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208.

Gollmann, D. (2011). *Computer Security*. Wiley, 3 edition.

Groth, J. (2016). On the size of pairing-based non-interactive arguments. In *Advances in Cryptology – EUROCRYPT 2016*, pages 305–326. Springer.

Jones, M., Bradley, J., and Sakimura, N. (2015). Json web token (jwt). Technical Report RFC 7519, IETF.

Liang, J., Hu, D., Wu, P., Yang, Y., Shen, Q., and Wu, Z. (2025). SoK: Understanding zk-SNARKs: The Gap Between Research and Practice. In *Proceedings of the 34th USENIX Security Symposium (USENIX Security 2025)*. USENIX Association.

Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

M'Raihi, D., Machani, S., Pei, M., and Rydell, J. (2011). Totp: Time-based one-time password algorithm. Technical Report RFC 6238, IETF.

Parno, B., Howell, J., Gentry, C., and Raykova, M. (2013). Pinocchio: Nearly practical verifiable computation. In *IEEE Symposium on Security and Privacy*, pages 238–252.