Título: Modelagem e Análise Formal para a Segurança Cibernética em Redes de Internet das Coisas

Proponente: Leandro Dias da Silva (leandrodias@ic.ufal.br), Álvaro Álvares de Carvalho César Sobrinho (alvaro.alvares@ufape.edu.br)

Descrição

Um dos objetivos com este projeto é propor soluções para segurança cibernética (por exemplo, protocolos e arquiteturas) e desenvolver modelos formais que viabilizem diferentes análises utilizando técnicas tais como a verificação automática de modelos (model checking) [1]. Nesse contexto, a modelagem e a verificação formal são abordagens práticas para documentar soluções, gerar evidências sobre cenários problemáticos, definir estratégias de mitigação e verificar requisitos de segurança [2,3]. Além disso, pode-se analisar formalmente soluções já existentes na literatura. Isso inclui a análise formal de protocolos, como o 5G-AKA e o EAP-AKA, bem como soluções voltadas à verificação de requisitos de segurança em redes móveis de quinta geração, especialmente no contexto de sistemas conectados e da Internet das Coisas [4,5,6,7]. Assim, neste projeto, será investigado como modelos formais podem ser utilizados para garantir o cumprimento de requisitos de segurança e identificar vulnerabilidades e ameaças em cenários de segurança cibernética, 5G e Internet das Coisas. Ao estudar soluções existentes, os resultados poderão ser apresentados na forma de relatos detalhados sobre as vulnerabilidades encontradas e acompanhados de propostas de mitigação.

Referências

[1] D. Valadares, A. Sobrinho, A. Perkusich, and K. Gorgonio, “Formal Verification of a Trusted Execution Environment-based Architecture for IoT Applications,” IEEE Internet of Things Journal, vol. 1, p. 1, 2021.

[2] X. Li et al. “A Model-Driven Security Analysis Approach for 5G Communications in Industrial Systems,” IEEE Transactions on Wireless Communications, vol. 22, no. 2, pp. 889–902, Feb. 2023.

[3] V.-L. Nguyen et al. “Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges,” IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2384–2428, Fourth Quarter 2021.

[4] S. Ji and A. Kumar Mishra, “5G Security Issues, Challenges and Solutions Against DDoS Attacks: A Survey,” in 2024 2nd International Conference on Disruptive Technologies (ICDT), Greater Noida, India, 2024, pp. 1422–1427.

[5] M. Mahyoub, A. AbdulGhaffar, E. Alalade, E. Ndubisi, and A. Matrawy, “Security Analysis of Critical 5G Interfaces,” IEEE Communications Surveys & Tutorials.

[6] V. Borges, A. Sobrinho, D. F. S. Santos, and A. Perkusich, “A Self-Sovereign Identity-based Authentication and Reputation Protocol for IoV Applications,” IEEE Access, vol. 1, p. 1, 2025.

[7] A. Sobrinho, M. Vilarim, A. Barbosa, E. C. Gurjão, D. F. S. Santos, D. C. G. Valadares, and L. Dias da Silva, “Challenges and Opportunities in Mobile Network Security for Vertical Applications: A Survey,” ACM Computing Surveys, vol. 1, p. 1, 2024.