3. Fighting Insider Threats, with Zero-Trust in Microservice-based, Smart Grid OT Systems

http://acta.uni-obuda.hu/Stanojevic_Capko_Lendak_Stoja_Jelacic_135.pdf

NEEDS CITATION**

1. **Microservices in Operational Technology (OT) Systems**: The paper discusses the benefits of implementing microservice-based architectures in OT systems, particularly in the smart grid sector. This approach can reduce upfront investment and maintenance costs.
2. **Cybersecurity Concerns in Modern System Architectures**: There is a hesitation among system operators to adopt these modern architectures, mainly due to cybersecurity concerns. The paper focuses on addressing these concerns by proposing mitigation strategies to reduce the likelihood of cyber-attacks.
3. **Development of a Comprehensive Threat Model**: The authors developed a threat model that encompasses both external and insider threats. This model uses Microsoft's STRIDE methodology to analyze threats at a service level in the smart grid context.
4. **Implementation of Zero Trust Principle**: The core of the proposed mitigation strategy is the zero-trust principle, which requires continuous authentication and validation of all users and nodes within the system, aiming to significantly reduce the risks of cyber-attacks.
5. **Risk Calculation and Mitigation**: The paper calculates the risks associated with each identified threat based on their impact and likelihood. It shows that the risks are significantly reduced when the proposed mitigation measures, based on the zero-trust principle, are applied.
6. **Analysis of Smart Grid OT Systems and Microservices**: The paper explores the traditional monolithic architecture of smart grid OT systems, discussing the benefits of transitioning to a microservices architecture, such as improved scalability and fault tolerance.
7. **Verification of Proposed Architecture Using STRIDE Methodology**: The proposed security controls and architecture are tested and verified using the STRIDE methodology. This involves identifying and measuring the risks associated with threat exploitation in the context of smart grid OT systems.

The paper is organized to cover related works, decompose the reference architecture, present the threat model and proposed mitigations, analyze components using STRIDE, and calculate risks for threat exploitation.