Breaking Supply Chain Threats: Threat Modeling for Post Quantum Cryptography in IOT & ICS

Ali Asgar Erinpurwala, Abhishta Abhishta, Roland van Rijswijk-Deij
University of Twente

BACKGROUND

From the Systematic Literature Review , we understand that migration to (PQC) Post Quantum Cryptography is not just a technical challenge, where just algorithms need to be optimized for constrained systems such as the ones used in Internet of Things (IOT) and Industrial Control Systems (ICS) but also an operational one.

HOW DOES THIS CONCERN SUPPLY CHAIN INDUSTRY

- **Quantum Computers, even though in their infancy, poses a "Harvest Now, Decrypt Later" threat, which means information intercepted today will be decrypted at the time when they become mainstream.**
- **Adversaries have been known to exploit third-party vulnerabilities, creating weak links if adequate security posture isn't maintained.**
- **Constrained systems face additional challenges mentioned in Fig.1 , making it convoluted to ensure optimal business uptime while mitigating high risk threats.**

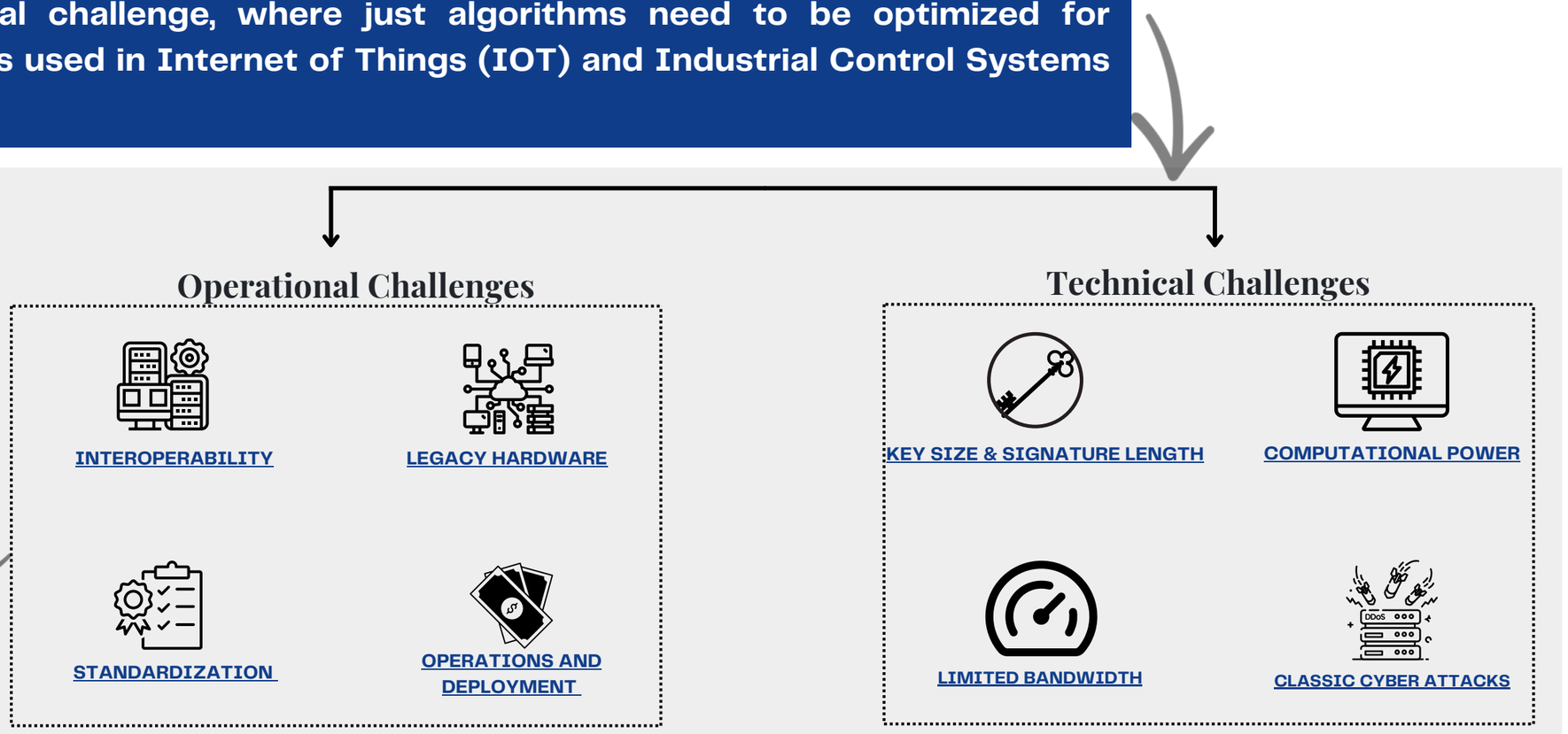

Fig.1 : Multidimensional challenges to PQC Migration for IOT & ICS devices

THE NEED OF AN HOLISTIC APPROACH

Fig 2 highlights the strong emphasis in the literature on practical PQC implementations across constrained environments with varying computational capacities.

In contrast, risk management remains the most neglected domain, underscoring the urgent need to prioritize threat modeling and risk assessment in PQC migration.

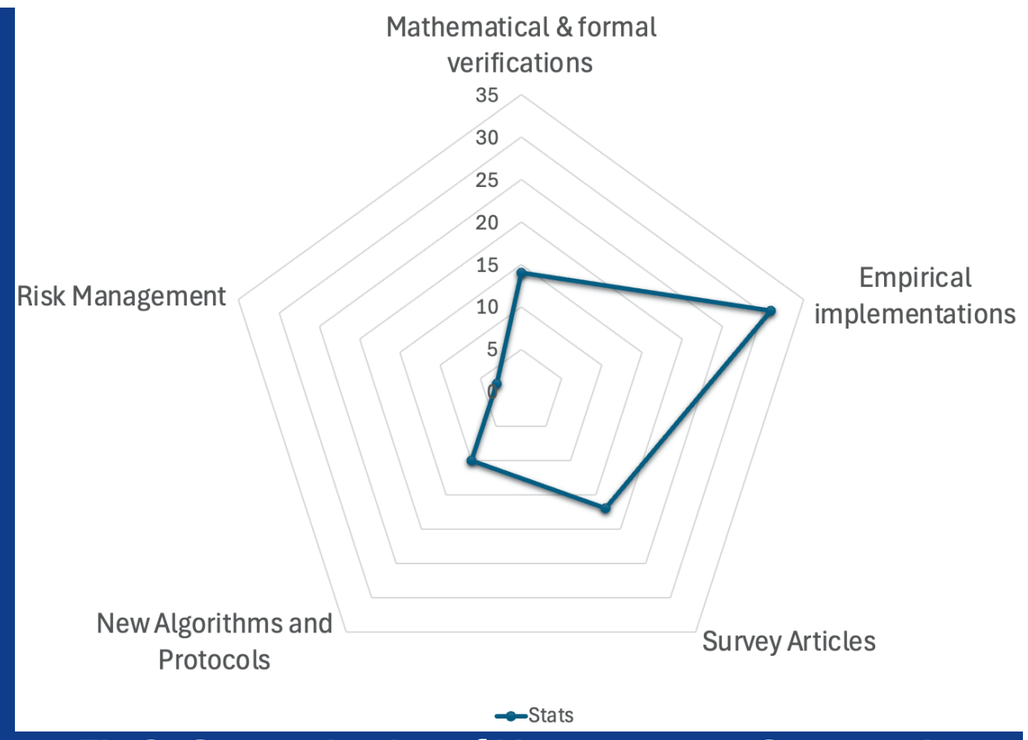

Fig.2 : Categorization of Literature over Systematic Review

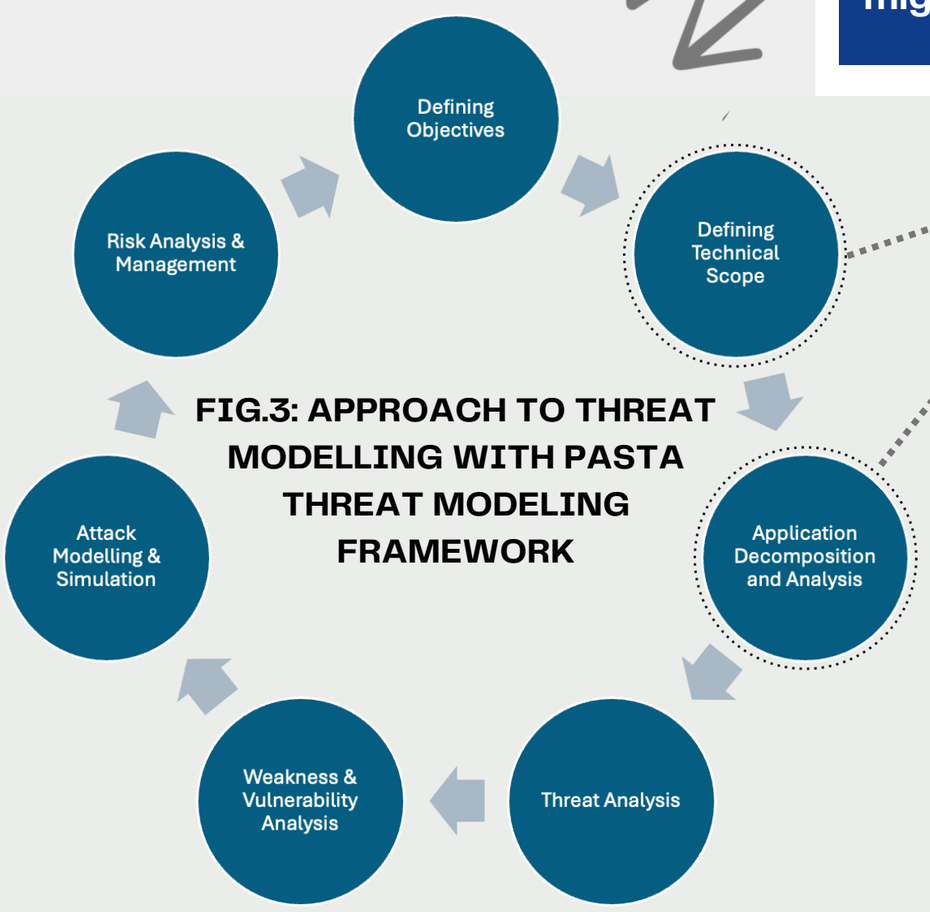

FIG.3: APPROACH TO THREAT MODELLING WITH PASTA THREAT MODELING FRAMEWORK

THE NEED FOR ESTABLISHING CRYPTOGRAPHIC BILL OF MATERIALS (CBOM) FOR IOT & ICS

1. **To structurize cryptographic inventories and understand their dependencies**
2. **To understand mapping of of cryptographic assets to enable visibility into trustzones and data flow in services**
3. **To understand hardware & software restrictions unique to industrial networks and systems**
4. **To facilitate the assessment of risk posture**

Lets's Connect & Exchange Ideas
Ali Asgar Erinpurwala
a.a.z.erinpurwala@utwente.nl

UNIVERSITY OF TWENTE.

DACS Design and Analysis of Communication Systems