Technical University of Munich

Thesis B.Sc.

Thesis M.Sc.

Towards Practical Post-Quantum Kerberos

Motivation

Quantum computing poses a significant threat to traditional asymmetric Kerberos authentication, particularly to public-key primitives used in PKINIT and related PKI-based extensions. For long-term security, exploring quantum-resistant authentication becomes essential to protect access and long-lived credentials. We need the adoption of post-quantum cryptography (PQC) in Kerberos. Quantum-secure configurations of the Kerberos protocol and performance trade-offs must address real-world deployment challenges beyond cryptography, including certificate lifecycles, PKI integration, KDC scalability, network overhead, and interoperability with existing Kerberos infrastructures. A deployment-oriented, principled analysis is needed to guide on variant selection. We also need to define PQC material management and mitigation strategies without sacrificing security guarantees.

Your Task

Your task is to review and synthesize various PQ-Kerberos protocol configurations. You need to develop a structured decision-making framework that justifies selecting among them based on real-world deployment criteria such as security, performance, scalability, and integration effort. Assess deployment feasibility in multi-user and multi-service environments, focusing on certificate management and KDC scalability. Using the chair's testbed to emulate a network of multiple nodes, propose concrete mitigation strategies for deployment frictions, including approaches to reduce communication overhead for larger PQC keys and signatures.

Requirements

- Strong interest and background in network security and quantum-secure systems.
- Basic knowledge of post-quantum cryptography and the Kerberos protocol.
- Programming languages: Python and C

Contact

Dominik Marchsreiter	dominik.marchsreiter@tum.de
Holger Kinkelin	kinkelin@net.in.tum.de
Marcel Kempf	kempfm@net.in.tum.de
Filip Rezabek	frezabek@net.in.tum.de