Toward a Quantum-Resistant, FIPS-Compliant Secure Operating System

Collin Blaine George
Independent Doctoral Research

June 19, 2025

Abstract

This dissertation explores the design, implementation, and impact of a secure operating system that is both FIPS 140-2 compliant and quantum-resilient. The work is motivated by the growing threat of quantum computing against classical cryptographic infrastructure, combined with the urgent need for hardened systems in critical and public infrastructure. The operating system is built on Ubuntu 22.04 LTS, using a combination of FIPS modules, hardened authentication mechanisms, and quantum-resistant cryptographic libraries (liboqs and oqs-provider). This system is architected to be auditable, reproducible, and deployable by organizations requiring high-assurance environments. The work is supported by fully scripted build processes, a GitHub-based change log, and is validated against U.S. NIST recommendations. The implications for cybersecurity, healthcare, and public safety are discussed in depth, offering a reproducible path forward for governments, healthcare systems, and infrastructure operators.

1 Introduction

The advent of quantum computing presents a fundamental challenge to modern cryptographic systems. As a result, institutions, enterprises, and governments must begin transitioning to quantum-resistant architectures. This research begins with the implementation of a secure, compliant, and hardened OS that incorporates state-of-the-art cryptographic libraries and practical system protections.

2 Objectives

- Build a production-grade, FIPS-compliant Ubuntu system.
- Integrate quantum-safe cryptography (Kyber, Dilithium, etc.).
- Enforce bootloader password and kernel lockdown.
- Ensure tamper resistance through full disk encryption.
- Enable secure, multi-factor user authentication.

3 System Architecture

We detail a hybrid dual-boot system with Windows 11 Enterprise and Ubuntu 22.04 LTS on bare metal. Ubuntu is customized with:

- FIPS kernel and OpenSSL FIPS mode enabled.
- GRUB2 bootloader with hashed password.
- Custom OpenSSL build linked to liboqs.
- Two-factor authentication using PAM + Google Authenticator.
- Audit logging, SSH hardening, and full disk encryption planned.

4 Results and Findings

The final prototype boots securely using a GRUB password, has a disabled GRUB shell, and performs FIPS-compliant crypto functions. liboqs successfully enables hybrid TLS (e.g., X25519+Kyber). Root shell access from GRUB recovery is disabled, and system modifications require multi-factor authentication.

5 Next Steps

- Implement LUKS2 disk encryption using XTS-AES-256 with integrity.
- Finalize logging (auditd, immutable logs).
- Expand to kernel module signing and verified boot.
- Publish research and ISO image on GitHub.

6 Conclusion

This work presents an independently developed reference for a hardened, quantum-secure Linux platform. It demonstrates the feasibility of aligning post-quantum cryptography, federal compliance, and practical usability in a single research-grade system.