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

Collin Blaine George
Independent Doctoral Research

June 29, 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.

Contents

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.

federal compliance, and practical usability in a single research-grade system.

7.1 Summary of Contributions

- A fully functional, hardened Linux system built with modern compliance standards.
- Integration of quantum-resistant cryptographic primitives (via liboqs).
- Development of scripts to automate compliance and security hardening.
- An academic and technical roadmap for future work and deployment.

7.2 Public and Academic Impact

- Provides a repeatable, standards-aligned security blueprint for organizations.
- Supports public infrastructure modernization and national cyber resilience goals.
- Lays groundwork for future doctoral research in cryptographic systems security.

A Script Listings

Scripts used for login hardening, PAM configuration, and GRUB lockdown are available at: `https://github.com/collingeorge/QUANTUMSECUREUBUNTU/tree/main/scripts`

B Installation ISO Build Instructions

See README documentation in the repository root.

C References

[1] NIST FIPS 140-2, https://csrc.nist.gov/publications/detail/fips/140/2/final

[2] DISA STIG for Ubuntu 22.04, https://public.cyber.mil/stigs/

[3] Open Quantum Safe Project, https://openquantumsafe.org

[4] Google PAM Authenticator, https://github.com/google/google-authenticator-libpam

[5] Ubuntu Security Documentation, https://ubuntu.com/security