Unit 8: Cryptography and Its Use in Operating Systems

Required Reading

Junestam, A. & Guigo, N. (2014) Open Crypto Audit Project Truecrypt Security Assessment.

Summary
The iSEC Partners report on TrueCrypt 7.1a, commissioned by the Open Crypto Audit Project, provides a comprehensive security assessment of TrueCrypt's bootloader and Windows kernel driver. The evaluation uncovered 11 vulnerabilities, categorized as medium, low, or informational severity, with no critical or high-severity issues identified. While no backdoors or malicious code were detected, the assessment highlighted weaknesses such as insufficient iteration counts for cryptographic key derivation, use of outdated or insecure functions, and lack of integer overflow protections. The report also noted issues with sensitive data exposure and code quality deficiencies, including inconsistent variable types and minimal commenting, which could hinder maintenance and security enhancements. High-level recommendations included modernizing the build environment, improving coding practices, and ensuring better error handling and documentation.

Reflection
This audit underscores the importance of maintaining rigorous development practices, especially for software handling sensitive data. TrueCrypt, while not exhibiting any intentional malice, fell short of contemporary coding standards, leaving it vulnerable to potential exploitation. The findings emphasize the criticality of adopting secure coding practices, robust cryptographic methodologies, and thorough documentation. The absence of high-severity vulnerabilities provides some assurance of its security, but the code's quality issues reflect broader challenges in sustaining open-source projects over time. This highlights the need for ongoing audits, community engagement, and modernization efforts to ensure such tools remain secure and effective in evolving threat landscapes.

TutorialPoint (2020) Cryptography with Python Tutorial.