Operating Systems Security in Sandboxing and Isolation Mechanisms

Tech Paper Proposal

CS 4310 Operating Systems

Prof. Gilbert Young

Devin Khun

Description

This paper will examine how modern operating systems implement sandboxing and process isolation as key security mechanisms. By comparing Linux (AppArmor, SELinux, seccomp-bpf), Windows (AppContainer, Defender Application Guard), and macOS (Sandbox, System Integrity Protection), the paper will highlight the technical approaches each OS uses to confine applications, restrict permissions, and mitigate attacks such as malware, privilege escalation, and kernel exploitation. The discussion will cover both strengths and limitations of these models, with attention to real-world vulnerabilities and the evolving threat landscape.

References

A. Niemi, "Survey of Real-World Process Sandboxing," *2024 35th Conference of Open Innovations Association (FRUCT)*, Tampere, Finland, 2024, pp. 520-531, doi: 10.23919/FRUCT61870.2024.10516417. keywords: {Surveys;Technological innovation;Linux;Focusing;Mobile communication;Servers;Security}.

Ligh, Michael Hale, et al. *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*. Wiley, 2014.

Zarif, Bin A. "Securing Operating Systems (OS): A Comprehensive Approach to Security with Best Practices and Techniques." *International Journal of Advanced Network, Monitoring, and Controls*, vol. 9, no. 1, 2024, pp. 100-111. *ProQuest*.