Project

[Author Name(s), First M. Last, Omit Titles and Degrees]

[Institutional Affiliation(s)]

Author Note

[Include any grant/funding information and a complete correspondence address.]

The paper is intended to cover a detailed review of operating system security. Operating system security is a fundamental concern for secure e-commerce and cyberspace. The vulnerable operating system ultimately impacts the overall application and services running on a device. Common computers and devices do not meet the requirements of a secure operating system. Computer architectures nowadays lack built-in mechanism for security policy enforcements because they are mainly based on a one-shot approach. That means either all the services and accesses are blocked, or all are granted. The reasons behind this behavior can be understood by decision-making protocols of the majority of commercial operating systems, which are based mainly on user identity and ownership.

One of the basic security criteria for the operating system is mandatory security which is “a built-in mechanism or logic within the operating system (often called system security module or system security administrator) that implements and tightly controls the definition and assignment of security attributes (Yang & C.Q, 2003)”. This criterion is central to the vulnerability-free operating systems. Conventional systems do not address criteria related to security, such as the trustworthiness of programs and operations. Mainstream operating system mechanisms, despite the claims, provide inadequate application security, which is based on user identity information. Hence it is needed to tackle application vulnerabilities and threats using Kernal level controls. This is one doable and effective way to secure operating systems.

The paper is intended to extensively explain possible security issues using conventional operating systems with details of various levels of security levels, including D, C1, C2, and B2, until A1, which is considered as the most secure level, where most operating systems are secure upto C2 or below. The paper will also cover a recent case study that provides secure operating system controls on kernel level and is built using the Linux based approach. It works by assigning mandatory access controls to ordinary computer systems and ensure kernel-level security.

**References**

Yang, C. Q. (2003). Operating System Security and Secure Operating Systems. *SANS Institute*.

Hsiao, D. K., Kerr, D. S., & Madnick, S. E. (1978, November). Operating system security a tutorial of current research. In *The IEEE Computer Society's Second International Computer Software and Applications Conference, 1978. COMPSAC'78.* (pp. 220-228). IEEE.

Masaki, H. A. S. H. I. M. O. T. O. (2013). A Survey of Security Research for Operating Systems. *情報セキュリティ総合科学*, *5*.

Balfe, S., Lakhani, A. D., & Paterson, K. G. (2005). Securing peer-to-peer networks using trusted computing. *Trusted Computing*, 271–298.

Zhao, M. X. (2015). Research on Operating System Security Technology. *Applied Mechanics and Materials*, *703*, 294–297. Trans Tech Publ.