World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:17, No:05, 2023

A Formal Verification Approach for Linux Kernel Designing

Authors : Zi Wang, Xinlei He, Jianghua Lv, Yuqing Lan

Abstract : Kernel though widely used, is complicated. Errors caused by some bugs are often costly. Statically, more than half of the mistakes occur in the design phase. Thus, we introduce a modeling method, KMVM (Linux Kernel Modeling and verification Method), based on type theory for proper designation and correct exploitation of the Kernel. In the model, the Kernel is separated into six levels: subsystem, dentry, file, struct, func, and base. Each level is treated as a type. The types are specified in the structure and relationship. At the same time, we use a demanding path to express the function to be implemented. The correctness of the design is verified by recursively checking the type relationship and type existence. The method has been applied to verify the OPEN business of VFS (virtual file system) in Linux Kernel. Also, we have designed and developed a set of security communication mechanisms in the Kernel with verification.

Keywords : formal approach, type theory, Linux Kernel, software program
Conference Title : ICSME 2023 : International Conference on Software Maintenance and Evolution
Conference Location : Barcelona, Spain
Conference Dates : May 22-23, 2023