TECHNISCHE UNIVERSITÄT DRESDEN

Faculty of Computer Science Institute of Systems Architecture, Chair of Operating Systems

Task for the preparation of a studienarbeit

Course:	Elektrotechnik (Diplom)
Name:	Yaoxin Jing
Matriculation number:	4838882
Title:	System call mechanisms avoiding privilege transition

Along with the steady performance improvement of peripheral devices like SSDs and RDMA network adapters, the operating system kernel now makes up for a significant share of the overall I/O latency and may introduce throughput limitations. The complex structure of the kernel is one of the main sources for this software overhead. Hence, in order to achieve better latency and throughput characteristics, system designers may choose to bypass the kernel completely when issuing I/O requests.

Kernel bypassing however renders secure sharing of devices difficult, since no centralised and trustworthy entity controls the operations issued by applications to the hardware, whereas the devices themselves mostly lack sufficient isolation mechanisms. Re-unifying low-overhead device access and multi-tenancy on modern high-performance hardware could be achieved by installing secure code snippets (*fastcalls*) into the application address space. The OS will trust fastcalls to access the hardware on behalf of the application and to adhere to OS-imposed control policies. However, in order for this approach to work, fastcalls must have unique access to hardware resources inside the application address space and must not introduce a significant overhead for accessing a device.

This thesis should answer the question of how to install fastcalls securely inside the user space application without exposing devices to unauthorised access. The thesis may consider limited modifications to a common CPU micro-architecture to provide the required security guarantees. This detailed analysis should then be used for designing and implementing a custom fastcall infrastructure. Finally, the evaluation should not only compare the new approach to existing solutions but also investigate applicability of several known CPU side-channel attacks and ways to mitigate them.

As part of this research, the thesis shall cover the following aspects:

1. In-depth analysis of the Linux system call implementation on the x86-64 micro-architecture
2. Implementation of a user-level fastcall mechanism
3. Latency comparison with existing kernel interfaces (custom system call as well as device drivers accessible via standardized system calls like ioctl)

Supervisors:	M. Sc. Maksym Planeta Dipl.-Inf. Till Miemietz
Issued on:	May 3, 2021
Due date for submission:	October 21, 2021

Digital signiert von TU Dresden CA
Ort:
Datum: 2021-05-31 11:23:49

Dr.-Ing. Michael Roitzsch (Acting Head of the Chair)
Supervising professor