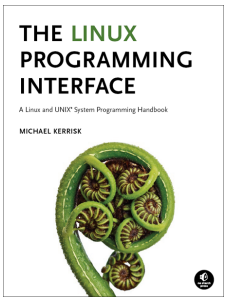
man7.org
Training and Consulting

Linux Secure Computing (Seccomp)

Course code: M7D-SECCOMP01

This course provides a thorough introduction to the Linux secure computing (Secomp) facility, a mechanism that can used to sandbox applications by limiting the set of system calls that they may perform.



Audience and prerequisites

The primary audience comprises designers, programmers, and systems administrators who are building, administering, or troubleshooting applications that employ seccomp as a sandboxing facility.

Participants should know how to log in to a Linux or UNIX system and be familiar with common shell commands. No particular programming experience is required.

Course materials

- A course book (written by the trainer) that includes all course slides and exercises
- A source code tarball containing example programs written by the trainer to accompany the presentation

Course duration and format

One day, with around 30-40% of the course time devoted to practical sessions.

Course inquiries and bookings

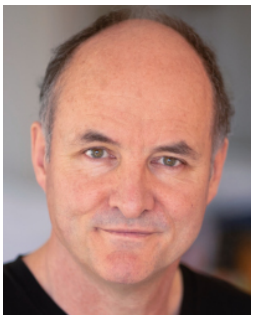
For inquiries about courses and consulting, you can contact us in the following ways:

- Email: training@man7.org
- Phone: +49 (89) 2488 6180 (German landline)

Prices, dates, and further details

For course prices, upcoming course dates, and further information about the course, please visit the course web page, `http://man7.org/training/cgroups/`.

About the trainer



Michael Kerrisk has a unique set of qualifications and experience that ensure that course participants receive training of a very high standard:

- He has been programming on UNIX systems since 1987.
- He has more than two decades of experience as a teacher and trainer, and first began teaching UNIX system programming courses in 1989.
- He is the author of *The Linux Programming Interface*, a 1550-page book acclaimed as the definitive work on Linux system programming.
- He has been actively involved in Linux development, working with kernel developers on testing, review, and design of new Linux kernel–user-space APIs.
- Since 2000, he has been the involved in the Linux *man-pages* project, which provides the manual pages documenting Linux system calls and C library APIs, and was the project maintainer from 2004 to 2021.

Linux Secure Computing (Seccomp): course contents in detail

Topics marked with an asterisk (*) may be covered, if time permits.

1. **Course Introduction**
2. **Seccomp**
   - Seccomp filtering and BPF
   - The BPF virtual machine and BPF instructions
   - BPF filter return values
   - Installing a BPF program
   - BPF program examples
   - Checking the architecture
   - Productivity aids (*libseccomp* and other tools)
   - Performance considerations
   - Applications, use cases, and further information
3. **Seccomp: Further Details (*)**
   - Caveats
   - Discovering the system calls made by a program
   - Installing multiple filters
   - Interaction with *fork()* and *execve()*
   - Extended BPF (eBPF)
   - Other filter return actions
   - Further details on BPF programs
   - Discovering seccomp feature support
   - Audit logging of filter actions