Operating Systems Lab
Jacobs University Bremen
Dr. Jürgen Schönwälder

Course: 320232
Date: 2016-10-27
Deadline: 2016-11-02

Problem Sheet #8

Problem 8.1: *credentials in the linux kernel* (1+1+1+1 = 4 points)

Read the Linux kernel documentation about how the kernel handles credentials and answer the following questions.

a) What are ’objects’ and ’subjects’ and what is an ’objective context’ and a ’subjective context’?

b) Tasks, like many objects, have a user ID (uid) and a group ID (gid). In addition, there is a effective user ID (euid) and an effective group ID (egid). How do these typically relate to an ’objective context’ and a ’subject context’?

c) How are credentials of a task represented in Linux? How can the credentials of the current task be obtained?

d) What is the proper way to update credentials?

Problem 8.2: *backdoor kernel module* (6 points)

Write a kernel module that implements a backdoor. An attempt to open a special non-existing file (by default /tmp/backdoor) should change the user ID and group ID credentials of the calling task to 0. The kernel module should have a parameter ’name’ that can be set in order to use a different name for the backdoor file. Explain (for example in a comment of your backdoor.c file) how a user space process can make use of the backdoor to obtain a root shell.