Dr. Matthias Grabert
Christian Ehrhardt

Systemnahe Software (SS 2002)

Abgabetermin 7.5.2002

Sandkasten (10 Punkte)

Als “sandbox” (oder zu deutsch Sandkasten) wird allgemein eine gesicherte Umgebung bezeichnet, in der ein nicht vertrauenswürdiges Programm ausgeführt werden kann, ohne über seinen Sandkasten hinaus Schaden anzurichten. Aufgabe diese Blattes ist es, einen solchen Sandkasten zu implementieren, der den Schaden durch eine fork-Lawine begrenzt. Dazu soll die Lösung von Blatt 1 entsprechend erweitert werden. Der Kindprozeß soll jetzt nicht mehr selbst irgendwelche (Enkel-)Kinder erzeugen, sondern (nach dem Eröffnen der neuen Prozeßgruppe) ein externes Programm ausführen. Dabei sollen natürlich auch die Argumente und das Environment kontrolliert werden können. Ein Beispielaufruf könnte dann so aussehen:

sandbox TZ=GMT /usr/bin/date

Dieser Aufruf sollte dann das Kommando date ohne Argumente aufrufen. Das Environment bestünde lediglich aus einem String nämlich “TZ=GMT”. Wenn alles funktioniert, dann sollte date die aktuelle Uhrzeit in der Zeitzone GMT (mitteleuropäische Sommerzeit minus 2 Stunden) ausgeben. Das Kommando, das ausgeführt werden soll, ist das erste Argument, das kein “=” enthält. Alles davor sind Umgebungsvariablen, alles dahinter sind Argumente, die mit übergeben werden sollen.
Der Vaterprozeß soll so erweitert werden, daß er, nachdem er seine Signale verschickt hat, auf die Terminierung seines eigenen Kindes wartet und dessen Exitstatus abfragt. Die Informationen, die sich aus dem Exitstatus gewinnen lassen, sollen dann in lesbarer Form ausgegeben werden (siehe wstat (3HEAD)).

Der Test

Um Ihr Werk gleich noch zu testen, soll noch ein zweites kleines Programm geschrieben werden. Dieses Programm soll zunächst seinen Kommandonamen und alle Argumente aus der Kommandozeile ausgeben. Anschließend soll überprüft werden, ob sich in seinem Environment eine Umgebungsvariable EXITCODE befinden, deren Wert eine Zahl ist. Falls das der Fall ist, soll das Programm mit dem entsprechenden Exitcode terminieren. Ansonsten soll es schlafen, bis es zwangsweise durch ein Signal beendet wird.