System Security Module: MCSSE-CYB-02
Constructor University Date: 2026-02-13
Dr. Jürgen Schönwälder **Due: 2026-02-20**

Problem Sheet #1

Problem 1.1: *buffer overflow exploit* (2+1+4+3 = 10 points)

Buffer overflows on an executable stack can be exploited to launch a shell via so called stack smashing attacks. Stack smashing attacks are specific to machine architectures since instruction set architectures differ in how they manage function calls the the stack. Furthermore, the attack code to launch a shell is specific to the targeted operating system.

You task is to develop a buffer overflow exploit for either an ARM CPU or a RISC-V CPU running a Linux kernel. Use a suitable virtual machine to develop and test your code.

a) Write shellcode (in assembler) targeting the selected CPU architecture and a Linux kernel. Ideally, your shellcode does not contain any NUL bytes. Automate the compilation of the shellcode using a suitable Makefile.

b) Write a program with a buffer overflow that can be exploited.

c) Generate attack code from the shellcode that can be be sent to the victim in order to launch the attack. Automate the construction of the attack code using a suitable Makefile. Demonstrate that the attack code is successful.

d) Explain and demonstrate how your solution works in a class meeting.