CSL373/CSL633 Minor 1 Exam
Operating Systems
Sem II, 2014-15

Answer all 6 questions Max. Marks: 32

Unix System Calls

1. Write the pseudo-code for a program ‘cp’ that takes two command-line arguments, say input-file and output-file, and copies the input file to the output file. [3]

Syntax:
$ cp ifile ofile

Code for cp:

```
void main(int argc, char **argv)
{
   // your solution goes here. use UNIX system calls to implement the functionality.




}
```

2. Consider the following function:

```
int32_t global;

int32_t foo(int32_t a, int32_t *b) {
  int32_t c;

  c = global + a;

  return *(b + c);
}
```

Assume that the variable global is allocated at a global address 0x12345. Write the assembly code for this function, with proper comments on which assembly code lines are implementing which C statement. Assume GCC calling conventions. You will need to be careful about properly naming all variables and arguments (e.g., using global addresses, stack offsets or frame pointer offsets), use proper opcodes and addressing modes, obey caller and callee-save conventions, etc. It is okay to not be exactly correct in the use of x86 opcodes, but the general layout of the code and its logic should be correct. [6]

3. How does the OS ensure through segmentation that one application cannot access another application's address space in the following situations: [10]

A. The application tries to write to the physical address of the other application.
B. The application tries to modify the segment register
C. The application tries to overwrite GDT entries
D. The application tries to lower its privilege-level (i.e., tries to gain supervisor privileges).

4. The instruction to load the Interrupt Descriptor Table Register (IDTR) is “lidt” and is a privileged instruction, i.e., it can only be executed in privileged mode. Assume that it was possible to execute this instruction in user mode by an untrusted user process. Show an attack using this additional (hypothetical) capability, whereby:

A. A user process can crash the machine.
B. A user process can read the memory contents of another process.

You should show the steps that the user process should follow to launch this attack in as much detail as possible. [8]

5. Assume a memory access latency of 100ns, and a 2-level page table hierarchy on 32-bit x86. What should be the TLB hit rate to ensure that the average memory access latency is 102ns. Assume there are no instruction/data caches in the hardware. [4]

6. Currently, the physical OS lectures repeat much material that is already present in the video lectures (let's call the current format, format A). We are contemplating a new format (say format B), where we assume that you have already listened to the corresponding video lecture before coming to the physical lecture, and spend the physical lecture time in quickly reviewing the material, question-answer session, exercise-solving, and most importantly, discussing advanced concepts around that material. (We believe that many students already listen to video lectures in advance). This way, we think you can learn much more from this course. Note that the "advanced concepts" will not be a part of exam syllabus.

Would you prefer format A or format B? Why? Please be honest in your answer.

For example, answers like "I am neutral" or "I don't care because I will not attend physical lectures in either case", are perfectly valid honest answers and will fetch full marks for this question. An answer like "I would love to learn more advanced concepts, and so I like format B" is also a valid answer.

We will plan the future lectures of this course based on this survey. [1]