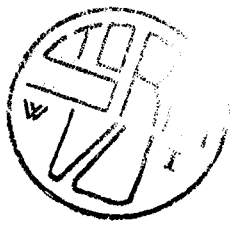

Internet Programming Exam

August 19th, 2003

Duration of the exam: 1 hour
This is a closed book exam: no documentation is allowed

---

1 Program Output

What will be the output of the following program? In which order will the output be printed?

```
#include <stdio.h>
#include <unistd.h>

int main() {
  int x;

  x = 0;
  if (fork()==0) {
    printf("foo\n");
    x = x + 1;
    exit(1);
  }
  else {
    wait(0);
    fprintf(stdout,"%d\n",x);
    execl("/bin/echo","echo","bar",NULL);
    execl("/bin/echo","echo","baz",NULL);
  }
  return 0;
}
```

(please turn the page for the second exercise)

2 A Voting Server

The goal of this exercise is to design a system which allows online voting (say, for a national Dutch election). Authorized voters are given a list of candidates to choose from. They must vote for one of the candidates from the list. At the end of the voting operation, an operator can request the result of the election, i.e., the number of votes that each candidate has received.

The voting application must work over the Internet: voters can vote from any machine connected to the Internet.

The voting application must be secured:

- Votes are secret: it must be impossible for an external attacker to find out who voted for which candidate.
- Only authorized voters are allowed to cast a vote.
- Each authorized voter can only vote once.

2.1 Server Structures

What are the available options for structuring the voting server? Explain how the server would be structured if you developed it using sockets, Sun-RPC, Java-RMI and Web technologies.

Write a **small** sketch of a server program based on sockets, which creates one child process per client.

Which server structure would you prefer for running the voting application? **Why?** Bear in mind that cryptographic operations usually require significant amounts of computation.

2.2 Securing the Voting Server

Which kind of security properties are required in this application? Which tools can be used? How can you implement them?

List all the messages transfered between the involved entities, and briefly describe their content.

— the end —