

University of Edinburgh
School of Informatics

Distributed Systems - Fall term 2010

Instructor: Dr. Richard Mayr

Course Projects (for level 11 students only!)

Assigned date: Nov. 4. 2010

Due date: Nov. 25. 2010. 4 PM at the ITO.

Choose ONE of the following two possible projects.

Project 1: Implement the Bully algorithm for leader election in Java.

Use (at least) 7 parallel processes P_1, P_2, \dots, P_7 . Each can spontaneously start the election. To make it interesting for observation, use a random number generator in each process to make it 'fail' with a certain probability in every step. A 'failed process' P_i should output "Process i has failed" and then never reply to messages from other processes.

Let the processes output status messages about what they are doing, e.g., "Process i requests permission from Process j ", or "Process i announces his leadership to Process j ", or "Process i recognizes Process j as leader", etc. Thus you obtain a protocol of what has happened in a run of the algorithm.

Deliverables:

1. The Java code: Ready to compile (with javac from the command line) and to do some test runs. To be submitted electronically with the 'submit' command.
2. A brief description of your program, design decisions (e.g., failure rates, timeouts), documentation, etc. (1-2 pages). Protocols of some test runs (at least 3 different outcomes). To be submitted **on paper at the ITO.**

Project 2: This is about Chapter 10 (Peer-to-Peer Systems) and Section 7.4.3 (Security) in the course text (Coulouris, Dollimore, Kindberg), as well as new material on the web. Answer the following two questions (in some detail).

1. Explain how using the secure hash of an object to identify and route messages to it ensures that it is tamper-proof. What properties are required of the hash function? How can integrity be maintained, even if a substantial portion of peer-to-peer nodes are subverted?
2. TOR (www.torproject.org) and I2P (<http://www.i2p2.de>) are two projects with the goal to provide anonymity on the Internet.

Theory: Describe the main differences between these two systems. Are there certain kinds of attacks against which one system is more secure than the other? If so, which ones, and why?

Practice: Try out both systems yourself and describe (briefly) your experience.

Deliverables: Answers to the questions (about 4-5 pages in total).