

7 Security (MGK)

- (a) An application process receives information via a UDP packet over a wired Ethernet LAN connection. If the packet carries a source port number below 1024, under which conditions can the information be trusted? [6 marks]
- (b) What is a *UDP-based amplification attack* and why are similar attacks far less practical via TCP? [6 marks]
- (c) Name and briefly explain *four* techniques that the designers of C compilers and operating system kernels can implement to reduce the risk of stack-based buffer-overflow attacks. [4 marks]
- (d) How can an implementation of the C function `strcmp()` cause a vulnerability to a side-channel attack, and how can this be mitigated? [4 marks]