Exercise 1: What advice would you give to employees to avoid being phished? Why might the advice not be viable in practice?

Exercise 2: When should a login with the correct username and password be rejected? Why?

Exercise 3: How could the Ucam-Webauth protocol and its implementation in the Raven system be improved?

Exercise 4: Pick two security protocols and explain why one succeeded in gaining traction while the other one failed to.

Exercise 5: You are responsible for the network of a company. How do you secure its multi-site network? The company has mobile workers and allows employees to use their own devices. Hint: A diagram may help.

Exercise 6: The NTP (Network Time Protocol) protocol defines an MON_GETLIST command which can be sent to NTP servers for monitoring purposes. Sending one single UDP packet can result in a substantial reply (details of up to 600 events may be returned). Since it can be trivial to forge the source of a UDP packet this allows Distributed Denial of Service (DDoS) attacks to be performed by setting the IP source address of the UDP packet to that of the intended victim – many gigabytes of DDoS traffic can be the result.

(a) Discuss the security economics of this situation, and suggest why there are difficulties in getting the owners of the NTP servers to alter the configuration of their systems.

(b) Another prevalent attack involves Domain Name Servers. An “open” recursive DNS resolver is asked to look up (one incoming UDP packet) a DNSSEC answer that is of substantial size. Once again forging the UDP source address allows a DDoS of an unsuspecting victim. Why will this issue be harder to address (hint: consider how attackers will choose the machines to send their packets to)?

Exercise 7: You are responsible for network security at a company. The website of the company is experiencing a DDoS attack. What should you do? You may make clearly stated assumptions about the company’s existing network.
Exercise 8: Computer Science Tripos Part II, 2009, Paper 8, Question 11

(a) Give four uses of anonymous communications other than censorship resistance. [4 marks]

(b) Explain the role of latency in anonymous communications. What limits or costs does low latency impose? [4 marks]

(c) Imagine you are a government censor, trying to identify which of your citizens are viewing forbidden websites through Tor.

(i) If you are able to wiretap the Internet connections of any 1% of the population, what effective capability does this give against Tor users? [4 marks]

(ii) If there are currently 1000 active Tor nodes, what extra capability would you acquire if you added a further 100 nodes under your control? Explain any assumptions you make. [4 marks]

(iii) If you are using Tor to escape censorship, how often should you change the circuit path you use? Explain your answer. [4 marks]

Exercise 9:

(a) Describe a scenario where an Internet censorship system would unintentionally block a legitimate website or other resource, when the blocking technique used is:

(i) DNS tampering

(ii) IP address blocking

(b) For each of your scenarios, describe how the blocking system could be improved to avoid the false positive, and state any disadvantages which would result.

Exercise 10: Early online anonymity systems were built around remailers for hiding email sender identities. Describe the characteristics of three different remailer types. What are the key differences that make web anonymity harder to achieve than email anonymity? Describe approaches to web browsing that offer similar characteristics to the three remailer types you gave earlier.

Exercise 11: Tor can either protect the anonymity of the client, or of both the client and server. Explain how the protocol works in both cases with reference to its telescoping path routing design.

Why is telescoping path routing used rather than classic onion routing (where the data is encrypted in advance for each hop)?

The Tor network offers anonymity and censorship circumvention. Explain how the Tor network could be attacked to reduce its effectiveness in each of these cases.