1) Traffic analysis has been one of the most important attacks. Theoretical protocols and implementation for anonymous Internet routing have been suggested (e.g., onion-routing, anonymizer, P2P anonymization etc.). Do some research on this topic and discuss this topic in the following aspects: do we need such kind of protocols and system? Will that be practical? Any legal implications?

2) Privacy issues about RFID have received extensive attention. Discuss how to protect privacy in electronic society.

3) Will we continue to develop faulty protocols that other people attack, or will we manage to develop a methodology for designing then right first time? What are the exact uses and limitations of formal methods (and other mathematical approaches, such as the random oracle model)? For your reference, you may think about the process how Microsoft CIFS protocol was broken (http://downloads.securityfocus.com/library/cifs.txt).

4) Is the man-in-the-middle attack realistic? List several scenarios to support your viewpoint. (A reference link: TCP hijacking with hunt http://www.giac.org/practical/gsec/Bhavin_Bhansali_GSEC.pdf)