UNIVERSITY OF DUBLIN

TRINITY COLLEGE

FACULTY OF ENGINEERING, MATHEMATICS & SCIENCES

SCHOOL OF COMPUTER SCIENCE & STATISTICS

MSc in Computer Science Trinity Term 201**4**
CS7453

Security of Networks and Distributed Systems

CS7053

Date	**Location**	**Time**
TBD	**TBD**	**TBD**

Dr. Stephen Farrell

Instructions to Candidates

Please attempt 3 questions.
All questions carry equal (33) marks.

Question 1. (33 marks)

You are a senior software developer in a large software company tasked to produce a security review process for a new product development group that has just been established. The group will be developing web services based applications for the healthcare market, specifically for hospitals, including handling of sensitive (patient) data. The security review process will be followed by designers and developers. You cannot expect that all people in the group will be familiar with security, and they will be under constant time-pressure to produce product deliverables. For the purposes of the answer, you can assume whatever general software development methodology you like is to be used (but do briefly describe that if its necessary to understand your answer).

(a) Outline the security review process you would initially suggest, and how it fits with the general software development methodology you select. (15)

(b) How would you get from your initial suggestion for a process to a final, signed-off security process to be followed by the group? Describe the actions you would take and the interactions with others you would expect to occur before you get that final sign-off. (10)

(c) How would the security review process be maintained over time in order to handle changes to the group's activities, the legal and the business environment? (8)

Question 2. (33 marks)

(a) For any real-world Internet key exchange protocol (e.g. TLS, S/MIME, IPsec, Kerberos) describe the key management and application data protection aspects of the protocol in detail, including a description of the common failure/error cases that might occur in typical uses of the protocol. (15)

(b) What are the main issues that arise with very large scale deployments of your chosen protocol ? (10)

(c) Describe the challenges in developing a constant runtime version of your chosen protocol in order to thwart timing attacks? (8)

Question 3. (33 marks)

You are designing a sports commentary system initially for the 2014 soccer world cup, but generally applicable to any large sports event. The system supplies running text and voice (e.g., mp3) commentary on matches in progress. The system is intended to be syndicated to many web sites and, in particular, is intended to support online gambling markets where bets of many sorts may be occurring, e.g. time of first goal, time/number of first yellow card etc. Conceivably, the amount of money changing hands could be sufficient to motivate attempts to attack the system. Given the interest in the world cup, the system has to be designed to be highly scalable, being able to cater for up to tens of thousands of syndicated sites.

(a) Provide an outline design for the system, with an emphasis on the security aspects. Include a network diagram. (15)

(b) Clearly your system cannot counter every possible threat whilst remaining usable and scalable. Describe one threat that your system does not counter, say why your system includes no countermeasure for this threat, and outline some operational or other ways of countering the threat. (10)

(c) How could potential customers or users of the system (e.g., gamblers or bookmakers) satisfy themselves that the system is secure and honest? (8)

Question 4. (33 marks)

(a) Describe three main threats that firewalls are designed to mitigate, and (in the abstract) how a firewall mitigating each threat described would be configured. (15 marks)

(b) How would you test that the set of firewalls in a large enterprise (say 1000 firewalls distributed world-wide) are properly configured? (10 marks)

(c) Describe common mis-configurations of firewalls and in each case indicate the kinds of expoit that such mis-configuration enables. (8 marks)