UNIVERSITY OF DUBLIN

TRINITY COLLEGE

FACULTY OF ENGINEERING, MATHEMATICS & SCIENCES

SCHOOL OF COMPUTER SCIENCE & STATISTICS

MSc in Computer Science Hilary Term 2013
CS7053

Security of Networks and Distributed Systems

Date	**Location**	**Time**
XX April 2012	**XXXX**	**XX**

Dr. Stephen Farrell

Instructions to Candidates

Please attempt 3 questions.
All questions carry equal marks.

Question 1. (33 marks)

A games company are planning to migrate their previously off-line single-person game to an on-line multi-player game, with the usual multi-player features (messaging, trading game items, player to player battles, non-player characters etc.). The company are planning to have game servers located in various data centres (co-location sites) around the world to provide lower latency access for their users. The game software has been developed and tested and the new version will be released soon, and the company have done internal work on security. As on-line multi-player gaming is new to this company they have hired you, as a security consultant, to help evaluate the security of their new game release and platform.

a) Describe the most relevant risks (at least 3) you see, including consideration of their impact and likelihood of occurrence, and outline the countermeasures you would expect that the company have implmented to mitigate those risks. (18 marks)

b) What questions would you ask about the company's internal development processes and the operational processes of the hosting data centres? (10 marks)

c) After you've finished this contract, another similar, competing company hires you to do a very similar piece of work. How might you expose confidential information related to the first company in carrying out this second contract? Describe steps you would take to avoid exposing such confidential information. (7 marks)

Question 2. (33 marks)

(a) For any real 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 impact of the exposure of relevant secret or private keys. (15)

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

(c) Describe any side-channel (e.g. timing, power) attacks might be attempted against a naïve implementation of your chosen protocol? (8)

Question 3. (33 marks)

You are asked to (re-)design a national application system for students to use when applying for third-level grants. The system should allow the applicants (and/or their parents or guardians) to enter contact, educational and financial information relating to family income, and to track the process of their grant application. Staff are responsible for validating the information entered against exam results, university applications and tax systems and for approving or denying applications. Payments for successful applicants are to be transferred to the correct bank accounts in a timely fashion. Auditors are special users who can randomly check the processing of applications and who also produce anonymised statistics as to the operation of the system. There are also system administration users who have privileges to manage the system but who should not have access to personal information about applicants. The system is expecteed to handle high peak loads and is considered likely to be attacked.

(a) Outline the overall design for such a system (include a network diagram) and describe the security requirements you would propose the system must meet (10).

(b) Describe, in detail, the security solution you would propose to meet those requirements. (15)

(c) Having designed the system, you are then fired and decide to launch a denial-of-service attack that prevents the system working, but so that you could not be traced as the bad-actor. How would you go about doing this? (8 marks)

Question 4. (33 marks)

a) Describe the concept of a de-militarized zone (DMZ) and how that is used in typical enterprise networks. Desribe three security technologies that one can reasonably place in a DMZ? For each, describe some threats that that technology mitigates and how that is achieved. (18 marks)

b) Describe a realistic network that uses the technogies, described in part A and say what kinds of penetration testing you would attempt in order to determine if the network is sufficiently secure. (The meaning of “sufficiently secure” will depend on the kind of network you describe.) (10 marks)

c) Describe common mis-configurations of one of the technologies that you described in part A and the kinds of expoit that such mis-configuration enables. (7 marks)