UNIVERSITY OF DUBLIN

TRINITY COLLEGE

FACULTY OF ENGINEERING, MATHEMATICS & SCIENCES

SCHOOL OF COMPUTER SCIENCE & STATISTICS

MSc in Computer Science Hilary Term **2015**

CS7053/CS7453

Security of Networks and Distributed Systems

Date	**Location**	**Time**
April 20th	**LUCE UPPER**	**9:30am – 11:30am**

Dr. Stephen Farrell

Instructions to Candidates

Please attempt 3 questions.
All questions carry equal marks.

Question 1. (33 marks)

A financial services software product company are highly distributed, with most of their 500 employees working from home offices and only a few people located in 5 small offices. Locations are scattered around the world, some better connected and some less well connected. The company want to introduce a new system for collaboration that supports employee meetings (video/audio/chat) and file storage, including source code control. The company are evaluating various service providers who offer solutions in this space and have tasked you do help them evaluate the security properties of the various bids they have received from service providers, including having you be a part of the team communicating with the bidders.

a) Describe the most relevant risks (at least 3) you see for the new system, including consideration of their impact and likelihood of occurrence, and outline the countermeasures you would expect that the company and/or their chosen service provider would need to impelment to mitigate those risks. (18 marks)

b) What other questions would you suggest the company ask about the service provider's systems and operational processes? (10 marks)

c) What countermeasures would you put in place to detect or prevent a dishonest developer employee from misbehaving? (5 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 how you would test which protocol features have been deployed in the wild. (15)

(b) What are the main barriers to deployment that affect your chosen protocol? (10)

(c) Desribe and justify how you think your chosen protocol might evolve in the coming deacde? (8)

Question 3. (33 marks)

You are asked to design a system for summoning and paying for taxis (like Hailo) or private car rides (like Uber). The system should have a web-based user interface as well as smartphone apps for end-users. Before the trip starts, the system provides the end-user with some basic information about the car/taxi and driver that are assigned to them. During or after the trip, the end-user can input comments on the driver/car. End-users can have an "account" that is pre-paid and billed for the trip, or can use cash or card-based payments. Drivers and taxi-company owners will have a separate interface that allows them to view statistical and payment information. The system is to be operated by a third party company who are not a taxi-company but who take a small commission for each ride that is arranged via the system.

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

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

c) Describe a non-obvious way in which you (as a system developer) might leave in place some feature that benefits you financially and that is hard to detect. (8)

Question 4. (33 marks)

a) Describe the architecture and key management hierarchy of DNSSEC. (15)

b) How will DNSSEC deployment impact on registrars, registries and applications? (8)

c) Describe ways in which the DNS can leak private information and how one might mitigate that with changes to DNS protocols, implementations and deployments. (10)