UNIVERSITY OF DUBLIN

TRINITY COLLEGE

FACULTY OF ENGINEERING, MATHEMATICS & SCIENCES

SCHOOL OF COMPUTER SCIENCE & STATISTICS

MSc in Computer Science Hilary Term **2014**

CS7053

Security of Networks and Distributed Systems

CS7053-1

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

Dr. Stephen Farrell

Instructions to Candidates

Please attempt 3 questions.
All questions carry equal marks.

Question 1. (33 marks)

A general insurance company who market motor insurance and life assurance are putting in place a new sales-support system for their sales staff. The system needs to handle sensitive customer data including financial and healtcare information but also deal with the fact that sales staff are mobile, often visiting customer sites (e.g. large employers whose employees they insure). Avoiding data loss and exposing customer personally identifying information (PII) is a criticial requirement, whilst at the same time ensuring that sales-staff have access to customer records they require to do their jobs. Sales staff will be given a new laptop specially provisioned for running the new system. Internally, the system is a web-based system that is actually operated by a 3rd party cloud provider. At the point where the insurance company have decided to use some 3rd party cloud provider but have not yet identified which one, nor all details of what the 3rd party will be required to provide, you are asked to do an initial risk analysis of their plans.

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 and/or 3rd party cloud provider would need to implment to mitigate those risks. (18 marks)

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

c) What countermeasures would you put in place to detect or prevent a dishonest member of the sales staff 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 interoperability between a new and an existing implementaion of your chosen protocol. (15)

(b) What are the main security failures that are likely to arise in implementations of 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 data-retention system for a social networking web site so they can respond to properly validated law enforcement requests for customer information. The web site uses a typical highly scalable web infrastructure with distributed front-end web servers and a distributed database as the backend for the web applications. All customer data that can be accessed is stored in the distributed database. The system needs to provide an interface where specially authorised operators can enter details of the requests received from law enforcement officials including how those requests have been validated. When a validated request is entered into the system a snapshot of all information relating to the customer(s) in questioncan then be copied into a special database. For some requests this snapshot process must be run periodically for some duration defined in the request. For some requests, it is allowed to inform the user of the law enforcement request, but for others the law requires that the request must be kept secret from the user. In all cases, the existence of the request and the associated snapshot data must be handled with extreme care, both from the confidentiality perspective but also in terms of preserving the chain of evidence.

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) Having designed the system and being a user of the social network in question, you want to know if you are ever the target for such surveillance. Describe ways in which you might leave in place some form of covert channel so that only you would know if you were being targetted but so nobody else would realise that. (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)