UNIVERSITY OF DUBLIN

TRINITY COLLEGE

FACULTY OF ENGINEERING, MATHEMATICS & SCIENCES

SCHOOL OF COMPUTER SCIENCE & STATISTICS

MSc in Computer Science Hilary Term 2012
CS7053

Security of Networks and Distributed Systems

EXAM SOLUTIONS

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 manufacturing company that are setting up a new web site to sell electronic components direct contracts you, as a security consultant, to carry out a risk analysis for the site and the associated payment and other processes. Previously the company has only dealt with distributors and never directly with end-users. Their goal is to out-source as much as possible of the work including web hosting, payments, the logistics for handling shipping of the products and customer service. The main product is a component that will be used in medical devices so a high level of assurance is required that processes are documented and followed. The company expect to sell thousands of devices per month. You can make any reasonable assumptions about how the web site works, but do make those clear in your answer.

(a) Describe the most relevant risks (at least 5) you see, including consideration of their impact and likelihood of occurrence. (18 marks)

(b) Describe the countermeasures (which may be physical or logical) you would recommend for the 3 highest priority risks and how deploying those countermeasures affects the overall risk analysis. (10)

(c) How and when should the company re-evaluate the security of their site after it has gone live? (5)

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 that security protocol is used by some real application. (15)

(b) What are the main potential Denial-of-Service (DoS) attack vectors that are created via the use of your chosen protocol? Describe those and potential countermeasures. (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 design the security subsystem of a federated system for medical researchers in various research institutions (universities, hospitals) to use to interact with health research data sources for example national cancer registries, hospital patient records and other large data-sets. The data-sets are also owned and operated by research institutions and government, but contain highly sensitive health-care records including personally identifying information.

The system should allow researchers in any institution to register and be granted access to only specific data relevant to their research. There are a set of special users ("approvers") who must manually approve new registrations. When a researcher issues a request for data, it will typically be necessary to filter the data so that only results that the researcher is allowed to see will be returned. For example a researcher might ask for the location and patient records of everyone in a large area who suffered from a particular disease, was under 45 years of age and who had a successful treatment. That query might be sent to multiple data-set holders, each of which runs its own system that decides what response to return.

Assume there are approximately 100 data-sets, 10,000 researchers and 100 "approvers" all of whom are distributed across a single country. Ideally, the researcher will in the end see a collated form of all results returned.

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

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

(c) Researchers are competitive too. Describe the various ways in which you, as a dishonest highly-competitive researcher, would attempt to abuse or game the system so as to make use of others work for your own benefit. (8)

Question 4. (33 marks)

(a) Describe three significant security issues with the Domain Name System (DNS) and say if those are mitigated via the use of DNS security (DNSSEC). (8)

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

(c) How will the deployment of DNSSEC affect end-hosts and applications running on the Internet and the management operations of registries and registrars? (10)