UNIVERSITY OF DUBLIN

TRINITY COLLEGE

FACULTY OF ENGINEERING, MATHEMATICS & SCIENCES

SCHOOL OF COMPUTER SCIENCE & STATISTICS

MSc in Computer Science Hilary Term 2011
CS7053

Security of Networks and Distributed Systems

Date	**Location**	**Time**
19th April 2011	**LB1.07**	**9:30am**

Dr. Stephen Farrell

Instructions to Candidates

Please attempt 3 questions.
All questions carry equal 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, 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 constant under 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.

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)

b) How would the security 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)

Ensure you read the full question before starting your answer as the various parts are related.

a) For any real Internet key exchange protocol (e.g. TLS, S/MIME, IPsec, Kerberos) describe the protocol in detail, including a description of the relevant configuration settings that an implementation would require. (15)

b) For your selected protocol, describe the main issues that would arise were it to be used in a large distributed network with some “normal” nodes but mostly consisting of many (i.e., millions), very small devices (e.g. motes) with limited processing power and memory and disrupted network connectivity. An example of such a network might be a country-wide seismic monitoring system but you can use any other example if that helps. (10)

c) Describe two changes you would recommend for your selected protocol that would mitigate some of the issues you identified in part (b) of this question. Be specific as to whether you consider each recommended change in something that could immediately be used, or whether your recommendation would be to experiment with the relevant change. (8)

Question 3. (33 marks)

You are asked to design an interpersonal communications system for staff from the International Monetary Fund (IMF) who visit countries in financial difficulty to negotiate IMF loans for that country. The system should support “instant” (e.g. jabber/XMPP) and store-and-forward (e.g. email) messaging as well as file transfer both between the IMF staff visiting a country as well as between them and staff at IMF headquarters. The messages, files and the computer systems involved are all considered highly sensitive and governments, hackers and financial-system actors can all be considered as potential attackers. Local network providers (e.g. in-hotel WiFi, GSM operators) are not to be trusted. In the context of a particular IMF visit to a country, only a small number of IMF staff should have access to the details (messages, files) of the negotiation. In your answer, you may skim over details of the messaging applications, but you must focus on the security services, mechanisms and components that are to be used.

a) Describe the security you would design for this purpose, focusing in detail on the security services and components. Your description should include security for the entire system, from the protection of the computer systems (e.g. laptops) to the applications and networks, and cover both application layer security functionality (e.g. confidentiality services) as well as other security components (e.g. audit, intrusion detection). Include system and network diagrams as appropriate. (15)

b) Describe how you would deploy and operate your system, that is, the processes required for adding and deleting computer systems and users and the processes you would follow to monitor the ongoing security of the system. Note that part (a) asks about the design of the system, but part (b) is concerned with operational issues. Your answers should not overlap significantly. (10)

c) You are an IMF system administrator based at IMF headquarters who is a citizen of a country being visited by an IMF negotiation team. Your government pay you to break into the system described above, in order to get information as to the negotiation position of the visiting IMF team. How would you go about that? (8)

Question 4. (33 marks)

a) Describe in detail the Domain Keys Identified Mail (DKIM) mechanism for associating an authenticated domain identifier with email messages. (15)

b) Describe the role that DKIM can play in countering phishing and SPAM and explicitly describe what DKIM *does not* provide in terms of countering phishing and SPAM. (8)

c) Briefly describe two other commonly used mechanisms that aim to mitigate problems caused by phishing attacks distributed via email. (5)

d) You are a spammer. Describe two ways in which you would you attempt to get your SPAM delivered to users in systems that have deployed DKIM signature verification and the other mechanisms you described in part (c)? (5)