QUESTIONS FOR CS7053 SECURITY EXAM 2010

Dr. Stephen Farrell

Question 1:

You are an independent security expert hired by a startup web services company that has just won a significant new contract with a major customer. The startup offer both installable/deployable products but can (they say!) also host deployments on behalf of their customers. The major customer is a mature business with a very structured way of handling information security. The startup are a startup and while they have thought about security for their products and service deployments, that has been done informally. Your task is to help the startup meet the requirements of the major customer. If it helps, you can use any reasonable startup/mature business scenario in your answer, e.g. a web merchant and a bank, a new social networking technology/site and a large ISP, etc.

(a) Describe what you consider are most likely to be the three most important generic security issues that you would expect to face in general in a situation like this? Note that the question here is not asking for a description of three specific technical vulnerabilities, but rather for the important process/company-level security issues that are likely to arise. (5 marks)

(b) Describe how you would determine the actual situation, (i.e. say how you would find out if and to what extent the particular issue applies), how you would set about mitigating each of the issues identified abouve assuming there is work to be done, and how you would determine that the issue has been sufficiently addressed. (15 marks)

(c) How would you, as a security professional, handle the situation where you suspect that the startup intends to lie to their major customer about some significant security issue? (5 marks)

Question 2:

(a) For any real Internet key exchange scheme (e.g. TLS, IKE, S/MIME), describe the protocol, specifically highlighing the main security features of the protocol and explaining why the designers chose these specific features. (For example, if a particular key derivation function is used, why is it done that way?) (10 marks)

(b) Discuss, in detail, the performance implications of your chosen protocol, both for clients and servers (or senders and recipients) covering a range of platforms and a range of scaling factors. (10 marks)

(c) Describe a way to modify the protocol, without seriously compromising security, that would result in improved performance in one of the situations you described in part (b) above. (5 marks)

Question 3:

The regulation of the financial industry has been in the news of late. You are asked to design the security aspects of a new system to be developed for a country's financial regulator that will be installed in each financial institution (“FI”) and will interface to that FI's internal systems, so as to give the regulator an online and immediate view of the FI's current activities.

Note: You can pick any country you like - if you happen to know some details of financial regulation in some country then its ok to use that country. The overall system is intended to report on the full range of FI activities (consumer and business banking, stock trading, interbank deals, insurance etc.) but for the purposes of answering the question you can limit the system as you see fit, for example, its ok if your answer only covers one of the above such as consumer banking. You should preface your answer with any assumptions along these lines that you wish to make.

(a) List and justify the 5 most important high-level security requirements that you would expect the system to meet. (5 marks)

(b) Provide an overview of the system, highlighting the security aspects of your design. Include diagrams as appropriate. (5 marks)

(c) How would you ensure that the deployed and running system meets the security requirements imposed at design time? (5 marks)

(d) How would you convince a third party (say a local parliament or Government committee) that the outputs from the system are trustworthy? (5 marks)

(e) It turns out you are dishonest and after the system has been runnning for a few years, you are paid a large sum of money by one FI so they can avoid or subvert the system. How would you set about doing this for them? (5 marks)