QUESTIONS FOR CS7012 SECURITY EXAM 2009

Dr. Stephen Farell/ Prof Vinny Wade

1. You are an internal IT security analyst for a consumer bank, which, like many banks these days, is facing market challenges. The bank's management wish to ensure that no further damage to the bank's reputation occurs and so have requested you to o a security review of their current consumer Internet banking offering.

   a) Describe a current consumer Internet banking operation, emphasising the security measures deployed, in both the customer-facing and internal parts of the system. (Note: you may use any real, or invented but realistic, consumer Internet banking operation with which you are familiar as the model when answering this question. It is not required however, that your description be exhaustive with respect to bank-internal systems; demonstrating an understanding of the server-side security issues in generic web applications is sufficient.)

   (10 marks)

   b) Given that management's goal is to reduce the risk of reputational damage to the organisation at this highly-sensitive sensisitve time, describe how you would approach carrying out a security analysis of the Internet banking operation you described above. (Your answer should cover both generic and system-specific aspects of risk analysis.)

   (10 marks)

   c) Banks are of course attractive targets for phishing attacks. How would you monitor general Internet activitiy so that you would have early warning that your bank is a current target of a phishing campaign? How should the bank react to that, when it occurs?

   (5 marks)

2. (a) For any real Internet key exchange mechanism (e.g. TLS, S/MIME, Kerberos), describe how that mechanism is used in some real application from the user interface down. For example, for HTTP/TLS your description might start with "The user clicks an https:// link." and would go on to detail that TLS handshake and application data protocols.

(10 marks)

(b) For the application you chose above, say how five errors can occur in the cryptographic mechanism that affect the user interface of the application? For each error considered, say how you think it *should* (as opposed to is currently) be presented to the user.

(10 marks)

(c) User testing indicates that many security error handling user interfaces merely triain users to click "ok" without thinking. Why is that and what would you do about it?

(5 marks)

3. You are asked to design an Internet survey system (e.g. like surveymonkey.com), but in this case only for use by law enforcement officials. The main function of the system is to allow users to setup and run simple surveys among targetted groups.

(a) What do you consider the 5 most important security requirements that the system must be designed to meet? (In each case, justify your selection.)

(10 marks)

(b) Describe your design for the overall system, specuifically calling out the aspects of the design that satisfy the requirements you stated above.

(10 marks)

(c) How might law enforcement officials abuse this system? How might you detect and react to such abuse?

(5 marks)