UNIVERSITY OF DUBLIN

TRINITY COLLEGE

FACULTY OF ENGINEERING & SYSTEM SCIENCES

DEPARTMENT OF COMPUTER SCIENCE

M.Sc. in Computer Science   Hilary Term 2008

Code & Name of Exam

Date of Exam   Location   Time of Exam

Name of Lecturer (Lecturers)

Attempt * questions
(all questions carry equal marks)

Question 1:

You are hired as an IT security specialist by a start-up "web 2.0" company developing a new social networking site similar to Flickr, Bebo or MySpace. The company have not previously thought much about security. Your first task for the company is to analyse what they've done so far and to suggest security-related improvements.
  (a) Name the top 5 security issues that you would first examine? For each, justify its inclusion on your top 5 list. (5)
  (b) For each of the top 5, how would you test whether or not the company's web site is sufficiently "secure"? (10)
  (c) For each of the top 5, if the test above "fails," describe the technical, procedural and/or policy countermeasures you would recommend to be put in place. (10)

(Note that the putative company are developing a web site, not a software product.)

Question 2:

  (a) Describe, in detail, a practical application data security and key management protocol (e.g. TLS, Kerberos, or IPsec). Include a description of how application data is protected, as well as key management exchanges. (10)
  (b) For your selected protocol, where and how should it be used by a company selling tangible goods (e.g. books, hardware) over the web? Include a network diagram, and consider that the overall system must scale so as to handle millions of users. (10)
  (c) What are the three most likely (note: most likely, not most impactful) threats related to the selected protocol that remain in the setup described in part (b) above? (5)

Question 3:

You are asked to design an Internet based system to allow citizens who are living abroad to vote in their national elections. Voters cast their votes for candidates in their "home" constituencies, e.g. a Dublin-registered voter living in New York might vote for candidates in the Dublin-central constituency. The number of voters involved is very small compared to the overall population at home, who vote using a traditional paper-based method. (Note: you can assume any realistic electoral system; it need not be the Irish one.)
  (a) Outline the system you would develop, emphasising security considerations. (Use diagrams where appropriate.) (10)
  (b) How would you validate the system before the election? (5)
  (c) Describe how the system would validate the votes cast, before, or as, they are counted, including any additional "sanity" checks you would put in place. (5)
  (d) You are a clever dishonest candidate with full knowledge of how the system works and lots of time and money. How would you attack the system? (5)

2007