1. Social Networks [2010 Paper 8 Question 11]
   (a) Social networking sites are becoming ever more popular, and many other sites now let users add each other as friends. Discuss the effect that social context has on
      (i) phishing;
      (ii) inference control;
      (iii) the market for privacy;
      (iv) community detection.
   (b) In what ways might social context be used to protect against harm online?

2. Domain Name System (DNS)
   Explain the security concerns with the DNS in terms of
   (a) confidentiality
   (b) integrity
   (c) authenticity
   (d) availability
   briefly outline a threat for each.

3. Phishing [2007 Paper 7 Question 3]
   A rapidly-growing online crime is phishing, in which victims are lured by an e-mail to log on to a website that appears genuine but that actually steals their passwords.
   You have been hired by a bank to help them harden their online banking service against phishing attacks.
   (a) Explain briefly the strengths and weaknesses of the following four possible countermeasures:
      (i) SSL/TLS client certificates issued to each customer;
      (ii) a hand-held password calculator issued to each customer;
      (iii) displaying a unique picture to each customer during the login process;
      (iv) requiring that large payments, or payments to new recipients, be authorised by telephone or SMS as well as online.
   (b) You are told that the budget will accommodate only two of the above options. Which two would you recommend, and why?

4. Inference Control
   Suppose that a social networking site such as Facebook wishes to expose information
about friendship statistics to researchers via Graph Search. For example, queries such as “What is the average number of friends for all users in the Cambridge network?” will be processed. To be safe, Facebook decides not to release the average friendship statistics for any query unless it pertains to a set of at least \( n \) user accounts, for, say, \( n \approx 10^3 \) (and, of course, fewer than \( N - n \) user accounts, where \( N \) is the total number of accounts).

Explain, in very specific terms, exactly how you could figure out how many friends your brother has in such a system.

5. **Passwords and Hashing**

To authenticate users it is considered a good practice for websites to store the hash of passwords rather than the passwords themselves in plain text. Consider the following issues related to this practice

(a) What is wrong with storing passwords in plain text?

(b) What is a salt value in this context and what role does it play? Should the salt be kept private?

(c) Differentiate between the security afforded in the following scenarios with respect to hashing passwords

   (i) each password is hashed and stored.

   (ii) each password is concatenated with a *fixed* salt before hashing and then stored.

   (iii) each password is concatenated with a *random* salt before hashing and then stored.

(d) Lets say a website stores passwords by adding salt and hashing them. Imagine you are given the hash of a password stored in the table, through black magic you are able to find a plaintext which also has the same hash i.e. \( H(s + p_{ori}) = H(p_{new}) \), where \( p_{ori} \) is the original password, \( s \) is the salt, \( p_{new} \) is the new plaintext that you have determined and \( H() \) is a cryptographic hash function. Since we are able produce the same hash can we use it to login to the website without even knowing the original password? Explain your answer and illustrate why this approach might work or fail.

(e) What are *Rainbow Tables* and how can they be used to attack the scheme illustrated? What are the counter measures against them, briefly discuss the approach taken by *bcrypt* and *scrypt* to defeat *Rainbow Tables*.

**Hint:**

http://security.blogoverflow.com/2013/09/about-secure-password-hashing/

6. **Security Policy Models**

In a military context, you have a BLP compliant system with a subject (= process)
A cleared to TOP SECRET and a subject B cleared to CONFIDENTIAL. A file X containing nuclear launch codes is labeled as TOP SECRET. Is it possible for A to transmit the content of X to B? If yes, how (and why would A want to do that)? If no, why?

7. Covert Channels
If the Bell-LaPadula system is fully implemented, a malware process which acquires root privileges will be able to read all files on the system, but not be able to write to any files which regular users can read. However, there are many other ways of conveying information. For each of the following possible covert channels, discuss how a signal process (high privilege) might communicate secret bits to an untrusted spy process, the rough efficiency of the channel, and what steps the system might take to eliminate or narrow the covert channel.

(a) Processor scheduling load
(b) Network traffic volume
(c) Power consumption
(d) System temperature
(e) Processor cache contents
(f) Virtual memory usage
(g) File system fragmentation

8. Replacing Passwords
Describe seven qualitatively different password replacement schemes and, for each, point out its most significant advantage over passwords and its most significant disadvantage. If two of your schemes have the same (best advantage, worst disadvantage) pair, they are not sufficiently different.