IY5512: Coursework 5

If feedback is required, coursework solutions must be submitted electronically via the course Moodle page. The deadline for receipt of submissions is 23:59 UK time on Friday 27/11/15. Coursework submissions should normally be in the form of a single pdf file. If you use Word, a free add-on to enable you to save a document in pdf format can be obtained from the Microsoft web site. Take care to ensure that you include your full name on the first page of your submission, the course number (IY5512), and the coursework number.

These questions are designed to test and extend your understanding of Part 5 of the course material.

1. What precautions should be taken when choosing passwords?

2. A password can be employed to authenticate a user to a remote server.
   a. Describe the risks to the confidentiality of the password arising both when it is communicated from the user to the remote server and when it is stored by the remote server.
   b. Indicate what measures can be used to reduce these risks.

3. What is wrong with the following 'challenge-response' user identification system?

   > Every user has a calculator capable of displaying 11 digits, and every also has a secret 10-decimal digit password. When a user wishes to authenticate him/herself to the system, the system generates a random 10-digit number and sends it to the user. The user (using the calculator) computes the sum of his/her secret password and the random number and returns it to the system, which then performs the same calculation (and hence verifies the user's identity).

4. How can the S/KEY system be attacked if a malicious party succeeds in impersonating the host?

5. Give a real-life example of the use of FIDO, and describe how it uses one of the standardised FIDO protocols.

6. Distinguish between user *identification* and identity *verification* schemes. List the five component modules of an architecture for a typical biometric system for personal identification, and briefly describe the purpose of each module.

7. Dual factor authentication is a practically important technique.
   a. What is meant by dual factor authentication and multi-factor authentication?
   b. Why can such an approach be advantageous?
   c. Give an example of such a scheme.

8. Think of a human (biometric) characteristic (not mentioned in the course notes) that might be used for identity verification for computer users. What sort of parameters would you measure?

9. What are meant by Type I and Type II errors in a biometric authentication system? Describe how this relates to threshold setting.

10. Describe how an identity management system based on the use of HTTP redirects can be attacked. How can the damaging effects of such an attack be reduced?

11. To what extent does the use of OAuth 2.0 for single sign-on protect user privacy?