

IY2760/CS3760: Coursework 3

Coursework must be submitted electronically, as an email attachment, to the following email address: me@chrismitchell.net.

Coursework submissions should normally be in the form of a single pdf file. It would greatly help me if you could name the attachment <lastname>_<first_initial>_3.pdf (e.g. Mitchell_C_3.pdf).

Take care to ensure that you include your full name on the first page of your submission, and also the course name and coursework number (i.e. 3).

1. PGP (Pretty Good Privacy) is a set of encryption and signature functions, a free version of which (GnuGP or GPG) is available for download on the Internet. It uses public key certificates but does not require the use of Certification Authorities (CAs). Describe some advantages and disadvantages of the PGP Keyring approach to public key management in comparison with the use of CAs.
2. What precautions should be taken when choosing passwords?
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. 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.
5. Think of a human characteristic (not mentioned in the course notes) that might be used for identity verification for computer users. What sort of parameters would you measure?
6. Within the various categories of malware, what is the main difference between worms and viruses? Name real-life examples of a worm and a virus, and briefly explain how these particular examples propagate themselves.

DEADLINE: 23:59, Tuesday 15th November 2011