

## IY2760/CS3760: Coursework 4

Coursework must be submitted electronically, as an email attachment, to the following email address: [me@chrismitchell.net](mailto: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>\_4.pdf (e.g. Mitchell\_C\_4.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. 4).

1. The following three access control mechanisms were discussed in the course notes:
  - access control matrices,
  - capabilities,
  - access control lists.

For each access control mechanism, describe the complexity of:

- determining authorised access during execution;
  - adding accesses for a new subject;
  - deleting all accesses for a particular subject;
  - determining all subjects which have access to a particular object;
  - creating a new object to which all subjects have access by default.
2. Give an advantage and a disadvantage of each of the following three types of non-repeating value, as used to counter replay attacks on authentication protocols (i.e. to provide ‘freshness checking’):
    - random numbers (unpredictable nonces),
    - sequence numbers (logical timestamps), and
    - clock-based timestamps.
  3. Suppose parties  $A$  and  $B$ , who share a secret key  $K_{AB}$ , use the following unilateral authentication mechanism (i.e. a mechanism which enables  $B$  to authenticate  $A$  but not vice versa):

$$A \rightarrow B: e_{K_{AB}}(t_A)$$

where

- $A \rightarrow B: X$  means that  $A$  sends  $B$  the message  $X$ ;
- $e_K(X)$  denotes the symmetric encryption of data  $X$  using the secret key  $K$ , where the encryption algorithm provides confidentiality and integrity protection; and
- $t_A$  is a timestamp generated by  $A$ .

Identify two possible types of attack (other than the use of a ‘weak’ encryption algorithm or loss of secrecy of the key).

4. Suppose parties  $A$  and  $B$  use the following unilateral authentication mechanism:

$$A \rightarrow B: t_A || s_A(t_A)$$

where

- $s_A(X)$  denotes a digital signature computed by  $A$  (using  $A$ 's private signature key) on data  $X$ ; and
- $t_A$  is a timestamp generated by  $A$ .

Suppose also that  $B$  possesses the public verification key of  $A$  (so that  $B$  can verify  $A$ 's signature). Identify two possible types of attack on this protocol (other than the use of a 'weak' signature algorithm or loss of secrecy of  $A$ 's private key). Compare these with the possible attacks on the protocol in the previous question.

5. Describe the Kerberos protocol for client-server authentication. Include a high-level description of the messages in the protocol, and describe the nature of the pre-existing relationships needed to support it.

**DEADLINE: 23:59, Tuesday 29th November 2011**