Distributed Systems 2005 (JMB) – Paper 8 Question 4 Solution notes

This question is on communication and access control for scalability

(a) (i) Define publish/subscribe communication.

<bookwork>

Publish/subscribe decouples message senders and receivers. Message topics/types (and contents/attributes) are first advertised by publishers.
Clients subscribe with a filter expression, indicating their specific interests.
3 Messages are multicast to interested subscribers only.

(ii) What are the advantages and disadvantages of offering publish/subscribe as the only communication service?

+ efficient routing algorithms for large-scale communication.
+ receivers need not know the names and addresses of all publishers, only the topic(attributes), typically by a yellow-pages style of service offered as part of the communications service.
+ publishers need not know the names and addresses of subscribers.
+ spam at the software level is prevented by control of who may advertise/publish/subscribe, see below.

- may sometimes want to send to a named principal.
- intra-domain communication may often be to individual names.
- may want to reply to a publication, either named or anonymised (as in a request to vote).
- may want to control who may subscribe. 7

(b) (i) Define role-based access control.

<bookwork>

* roles can reflect people's positions in an organisation, their functional responsibilities etc.
* services can indicate authorisation policy in terms of role names. 3

(ii) What are the advantages and disadvantages of using role names for access control and communication?

+ roles change less often than people come and go and change jobs/functions.

+ administration of people in roles is separated from that of service development and authorisation policy specification.

- if only role *names* can be indicated, only crude policy can be expressed.
  It may be necessary to know the names of individuals, to test for exceptions and relationships.
  e.g. X may not read my EHR
  e.g. doctors may read the EHRs only of their registered patients.

- if communication can only be to roles and not individuals this is again too coarse-grained. Some messages may need to be sent to specific individuals.
  e.g. duty-sergeant (cambs, cambridge-office, ...)
  e.g. duty-sergeant (sergeant-ID, ...)
  e.g. sales-manager (london, ...)

We therefore need the ability to specify individuals as well as role names.
This can be achieved by parametrised roles which is preferable to defining a huge number of roles. Without parametrisation a large organisation might
7 have many thousands of roles.

20