CMPSCI 677: Operating Systems
Homework 4
Sample Solution
Spring 2002

1. Suppose you were asked to develop a distributed application that would allow teachers to set up exams. Give at least three statements that would be part of the security policy for such an application.

   Answer —

   Obvious requirements would include that students should not be able to access exams before a specific time. Also, any teacher accessing an exam before the actual examination date should be authenticated. Also, there may be a restricted group of people that should be given read access to any exam in preparation, whereas only the responsible teacher should be given full access.

2. What is wrong in implementing a nonce as a timestamp?

   Answer —

   Although a timestamp is used only once, it is far from being random. Implementations of security protocols exist that use timestamps as nonces, and which have been succusfully attacked by exploiting the nonrandomness of the nonces.

3. Does it make sense to restrict the lifetime of a session key? If so, give an example how that could be established.

   Answer —

   Session keys should always have a restricted lifetime as they are easier to break than other types of cryptographic keys. The way to restrict their life-time is to send along the expiration time when the key is generated and distributed. This approach is followed, for example, in SESAME.

4. NFS does not provide a global, shared name space. Is there a way to mimic such a name space?

   Answer —

   A global name space can easily be mimiced using a local name space for each client that is partially standardized, and letting the automounter mount the necessary directories into that name space.

5. Taking into account cache coherence as discussed in Chap. 6, which kind of cache-coherence protocol does NFS implement?

   Answer —

   Because multiple write operations can take place before cached data is flushed to the server, NFS clients implement a write-back cache.

6. What calling semantics does RPC2 provide in the presence of failures?

   Answer —

   Considering that the client will be reported an error when an invocation does not complete, RPC2 provides at-most-once semantics.