Solutions to the
Third COSC 6360 Quiz
for Fall 2012

Jehan-François Pâris
jfparis@uh.edu
In PCC, which entity is responsible for defining the set of safety rules that will guarantee the safety of an extension? (5 points)
Answer

- The consumer
Nooks

- Why do Nooks wrappers replace all \textit{calls by reference} by \textit{calls by value and return}? (10 points)
Answer

- To delay kernel memory changes until the procedure terminates

**ALSO**

- Because the extension cannot modify the kernel address space outside its lightweight protection domain
Nooks again

- Give one reason for the *relatively high overhead* of Nooks (10 points)
Answer

- The TLB is flushed each time the kernel switches between protection domain
  - Must be done each time the page map changes
Lamport's Clocks

- A system of physical clocks consists of two clocks,
  - One that is fast and gains two minutes every hour
  - Another that is neither fast nor slow.
Lamport's Clocks

Assuming that the clocks are managed by Lamport’s physical clock protocol, what will be the time marked by each clock at 3 pm given that:

- Both clocks indicated the correct time at noon;
- The processors on which the clocks resides stopped exchanging messages at 1 pm; and
- Message transmission delays are negligible.

(2×5 points)
## Answer

<table>
<thead>
<tr>
<th>Actual Time</th>
<th>Fast Clock</th>
<th>Correct Clock</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:00 pm</td>
<td>12:00 pm</td>
<td>12:00 pm</td>
</tr>
<tr>
<td>1:00 pm</td>
<td>1:02 pm</td>
<td></td>
</tr>
<tr>
<td>2:00 pm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:00 pm</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Answer

<table>
<thead>
<tr>
<th>Actual Time</th>
<th>Fast Clock</th>
<th>Correct Clock</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:00 pm</td>
<td>12:00 pm</td>
<td>12:00 pm</td>
</tr>
<tr>
<td>1:00 pm</td>
<td>1:02 pm</td>
<td>1:02 pm</td>
</tr>
<tr>
<td>2:00 pm</td>
<td>2:04 pm</td>
<td></td>
</tr>
<tr>
<td>3:00 pm</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Answer

<table>
<thead>
<tr>
<th>Actual Time</th>
<th>Fast Clock</th>
<th>Correct Clock</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:00 pm</td>
<td>12:00 pm</td>
<td>12:00 pm</td>
</tr>
<tr>
<td>1:00 pm</td>
<td>1:02 pm</td>
<td>1:02 pm</td>
</tr>
<tr>
<td>2:00 pm</td>
<td>2:04 pm</td>
<td>2:02 pm</td>
</tr>
<tr>
<td>3:00 pm</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Answer

<table>
<thead>
<tr>
<th>Actual Time</th>
<th>Fast Clock</th>
<th>Correct Clock</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:00 pm</td>
<td>12:00 pm</td>
<td>12:00 pm</td>
</tr>
<tr>
<td>1:00 pm</td>
<td>1:02 pm</td>
<td>1:02 pm</td>
</tr>
<tr>
<td>2:00 pm</td>
<td>2:04 pm</td>
<td>2:02 pm</td>
</tr>
<tr>
<td>3:00 pm</td>
<td>3:06 pm</td>
<td>3:02 pm</td>
</tr>
</tbody>
</table>
BitTorrent

- What is the purpose of the *strict priority* rule for BitTorrent peers? (10 points)
- When does it apply? (5 points)
Answer

- In order to get complete pieces as quickly as possible

- Always

- It is the random first piece rule that only applies to new peers.
If you do not believe it

2.4.1 Strict Priority

BitTorrent’s first policy for piece selection is that once a single sub-piece has been requested, the remaining sub-pieces from that particular piece are requested before sub-pieces from any other piece. This does a good job of getting complete pieces as quickly as possible.
Lamport's clocks again

- What is the major disadvantage of *logical clocks* over *physical clocks*? (10 points)
Answer

- Logical clocks do not preserve the causality relation in systems where processes can exchange information through external events.
Kerberos

Assume that you are working on a new version of Kerberos that would encrypt all communications between the client and any service it is connected to. What would you use as a session key? (10 points)
Answer

- The shared secret session key $K_{c.s}$
  - Generated by TGS
  - Communicated to the client and the service
Encryption

- Bob knows the public key of Alice $K_{P,A}$ and knows that she knows his public key $K_{P,B}$. He sends her the following message:
  - “I am Bob. Please communicate with me using secret key 234ff08a79dce”
  and encrypts it with Alice public key. What did he do wrong? (10 points)
Answer

- He did not sign it with his secret key $K_{P,B}$
- Anyone else could have sent the message
SSH

- What should we try to know about a server before connecting to it through SSH? (10 points)
- What could happen otherwise? (10 points for a brief explanation)
Answer

- The public key of the server

- Otherwise any intruder could masquerade as the server by sending us a fake public key

- Masquerading with the true public key will result in little gain as long as the intruder does not know the secret key of the server