Solution to the Third COSC 6360 Quiz for Fall 2013

Jehan-François Pâris

jfparis@uh.edu

First question

- In the Kerberos system, which entities share these secret keys or passwords?
(5 points per correct line, no partial credit)

Answer

Secret	User's WS	Kerberos	TGS	Server S
User's password	__X__	__X__	______	______
Secret key of TGS	______	______	______	______
Secret key of server S	______	______	______	______

Answer

Secret	User's WS	Kerberos	TGS	Server S
User's password	__X__	__X__	______	______
Secret key of TGS	______	__X__	__X__	______
Secret key of server S	______	______	______	______

Answer

Secret	User’s WS	Kerberos	TGS	Server S
User’s password	__X__	__X__	______	______
Secret key of TGS	______	__X__	__X__	______
Secret key of server S	______	______	__X__	__X__

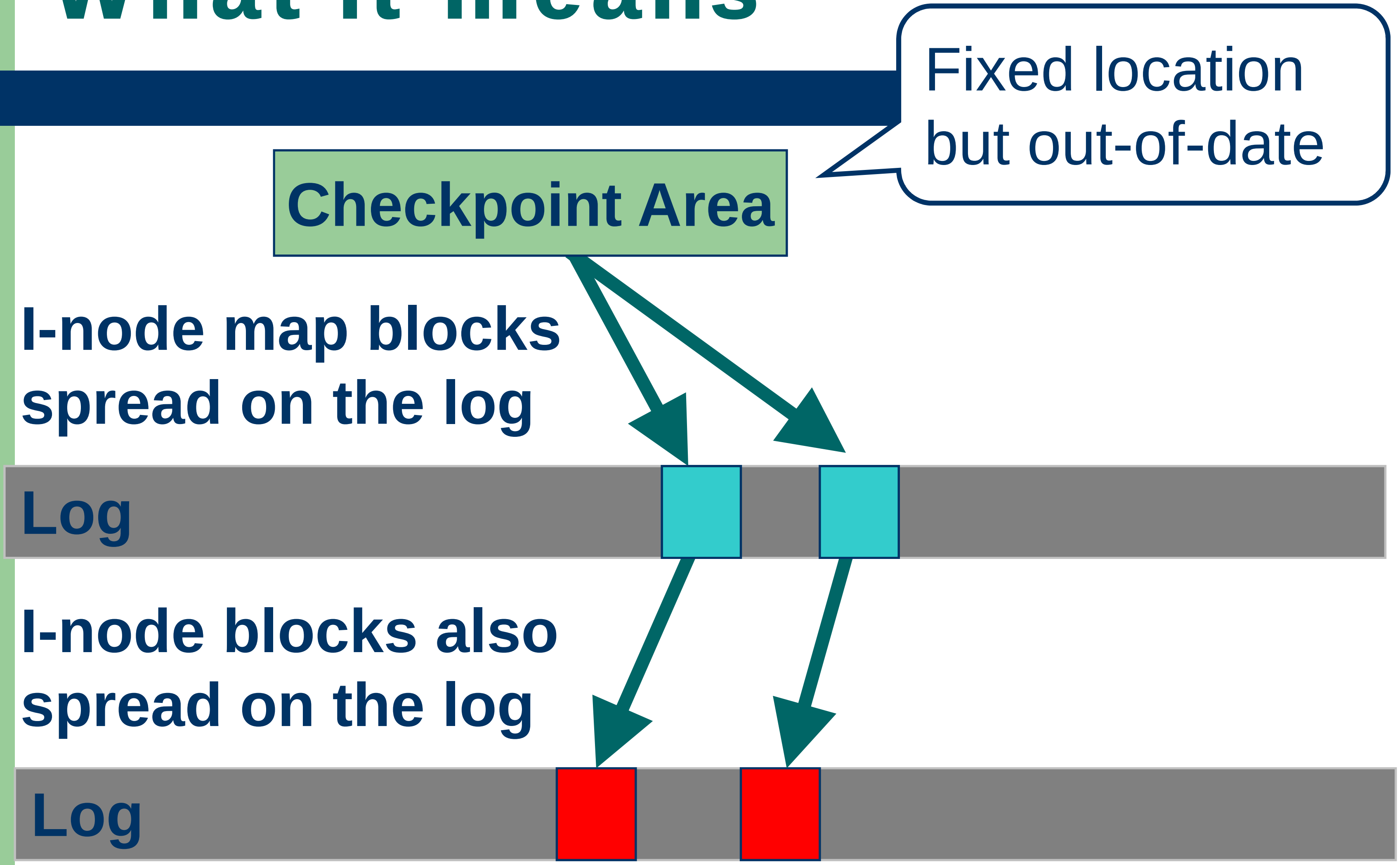
Second question

- What is the function of the ***i-node map*** in a log-structured file system? (10 points)
- Where and how is it stored on the disk? (5 points)

Answer

- The i-node map contains the ***addresses*** of the i-node blocks.
  - Required because i-nodes do not reside at fixed positions on the disk.
- The i-node map is stored ***on the log*** along with the data blocks, the directory blocks and the i-node blocks.
  - ***Not at a a fixed location!***

What it means



Fixed location but out-of-date

Checkpoint Area

I-node map blocks spread on the log

Log

I-node blocks also spread on the log

Log

Third Question

- Consider a RAID-5 array having four data blocks, namely, b_0, b_1, b_2, and b_3, and one parity block p per stripe
- Assuming that block b_3 suddenly becomes unavailable, how could you reconstruct its contents?

Answer

$$b_3 = b_0 \oplus b_1 \oplus b_2 \oplus p$$

Fourth question

- It would allow intruders to ***replay*** tickets of legitimate users

Fifth question

- What is the purpose of the BitTorrent ***rarest first*** rule? (10 points)
- When does it ***not*** apply? (5 points)

Answer

- The rarest first policy ensures that each downloader fetches first the pieces that most of its peers want.
- It does not apply to downloaders that have not yet downloaded their first piece.

Sixth question

- What is the purpose of ticket transfers in lottery scheduling? (10 points)
- Which problem do they solve? (5 points)

Answer

- Ticket transfers provide explicit transfers of tickets from one client to another
  - When a client waits for a reply from a server, it can temporarily transfer its tickets to that server
- They eliminate ***priority inversions***

Seventh question

- According to Shah et al., what is the main motivation for their ***randomized tit-for-tat*** policy? (10 points)

Answer

- Randomized tit-for tat lets each peer select neighbors at random at the beginning of every playback
  - Results in faster diffusion of new chunks among peers **OR**
  - Gives more free tries to a larger number of peers in the swarm to download chunks

Eighth question

- What are the main property and the main use of SHA-1 signatures?
(10 points)

Answer

- SHA-1 is a cryptographic hash function
- It guarantees that any change to the hashed data will (with very high probability) change the hash value
- It is used to verify the ***integrity*** of SSH packets