CprE 550:
Final Exam

Due on May 7, 2015

Instructor: Professor Yong Guan

Chenguang He

Contents

Question 1

(1) (5points) In the two-phase atomic commit protocol, each client has an uncertainty period after it has voted yes for a request (transaction) and is waiting for the final decision (commit or abort) from the coordinator. Can the client time out and unilaterally abort the transaction? Explain

Answer:

No, in order to abort the transaction, the client have to receive a message from the coordinator to notice the client to abort. If the client is time out, by the Two-Phase atomic protocol, the coordinator sends a rollback message to all client and each client stop the transaction and rollback using the undo log file, meanwhile, it release the holding resource and locks. After that, each client sends an ack to coordinator. Finally, the coordinator receive ack message from all clients, it undo the transaction.

Question 2

(2) (5 points) Given the read and write operations shown in the following Figure (a) and (b), please answer whether are (a) sequentially-consistent, (b) causally-consistent, and (c) FIFO consistent. Please explain your answer.

Answer:

(a) is FIFO consistency. Because the operations in single process P2 is in the order of W(x)b and W(x)c, it arrives in P3 and P4 with same order (b before c).

(b) is causal consistency. It is FIFO consistency, but it is stronger than FIFO, however it is weaker than sequential consistency, because the order of R(x)a R(x)b R(x)c in P4 and P3 are not same.

Question 3

(3) (10 points) What happens during each of the following operations in the following execution schedule of four transactions T1, T2, T3 and T4 accessing the three items A, B, and C? The concurrency control mechanism is time-stamp based. (Simply note ok if nothing special happens during the execution of a particular operation.)

Answer:
A: Max(rt) = 150, Max(wt) = 275
B: Max(rt) = 275, Max(wt) = 200
C: Max(rt) = 0, Max(wt) = 250

Question 4

(4) (5 points) In the release consistency model, acquire and release operations only need to be processor consistent. Why is this a sufficient condition for the shared variables to be FIFO consistent? What are the benefits of using release consistency as compared to sequential consistency?

Answer:

Q1: Because the FIFO consistency only make sure the order of write for shared variable in single process, it is good enough for acquire the variable. If we use other consistency, for example, the sequential consistency, it is too strong of the order of operations.

Q2: Sequential consistency is too strong restriction, it is inefficiency compare to release consistency. It slows the concurrent process.

Question 5

schedule	legal?	serializable?	A	B	2PL	result for timestamp
1234	Y	Y	3	2	Y	Y
3412	Y	Y	2	3	Y	Y
1342	N	N	1	1	N	NOT LEGAL t1 rollback
3124	N	N	1	1	N	NOT LEGAL t1 rollback
1324	N	N	2	2	N	N t1 rollback
3142	N	N	2	2	N	N t1 rollback

Question 6

(5) (10 points) Transactions T and U execute on a single server. In the table below, time proceeds from top to bottom, and relative position of operations indicates the relative order in which they were performed. State whether the execution below is possible in each of the following cases. If you answer no, provide a brief explanation. With read-write locking, the transactions acquire read lock when that is adequate.

(a) Exclusive locks are used with strict two phase locking, and all locks required by a transaction are acquired at the start of the transaction.

Answer:
No, At the beginning, transaction T acquires a shard lock on y and a shard locks on x, transaction U acquires an exclusive lock on z. When U do operation ”write(y,3)”, it have to acquire the lock on y. To acqiure it, U must wait for T commit. However, when T do operation ”c=read(z)”, T have to wait for U commit. It is in the Deadlock.

(b) Exclusive locks are used with non-strict two phase locking.

Answer:
Yes
T transaction can successfully unlock(y) and unlock(x), then transaction U continues.
(c) Read-write locks are used with strict two phase locking, and all locks required by a transaction are acquired at the start of the transaction.

Answer:
Yes, same to above, expect transaction U first lock and unlock then transaction Y lock and unlock

Question 7

(5 points) In Message 2 of the Needham-Schroeder authentication protocol, the ticket is encrypted with the secret key shared between Alice and the KDC. Is this encryption necessary? Please explain.

Answer:
Yes, it is necessary. Because an intruder can catch the message which contains the information: session key between A and B, information of A and B, intruder can make a masquerade of A and communicate with B.

Question 8

(5 points) Please do a literature survey on TCB, TPM, and SGX, in particular, what will we be able to do with SGX in secure distributed applications or systems? If possible, please use some examples.

Answer:
Intel SGX is a set of CPU instructions which can be used by applications to make a ”invert sandbox” of code and data. It has eight objective:
1. Allow application developers to protect sensitive data from unauthorized access or modification by rogue software running at higher privilege levels.
2. Enable applications to preserve the confidentiality and integrity of sensitive code and data without disrupting the ability of legitimate system software to schedule and manage the use of platform resources.
3. Enable consumers of computing devices to retain control of their platforms and the freedom to install and uninstall applications and services as they choose.
4.Enable the platform to measure an applications trusted code and produce a signed attestation, rooted in the processor, that includes this measurement and other certification that the code has been correctly initialized in a trustable environment.
5. Enable the development of trusted applications using familiar tools and processes.
6. Allow the performance of trusted applications to scale with the capabilities of the underlying application processor.
7. Enable software vendors to deliver trusted applications and updates at their cadence, using the distribution channels of their choice.
8. Enable applications to define secure regions of code and data that maintain confidentiality even when an attacker has physical control of the platform and can conduct direct attacks on memory.

In secure distributed application or system, SGX can help to enhance the secure of application by [8] Enable applications to define secure regions of code and data that maintain confidentiality even when an attacker has physical control of the platform and can conduct direct attacks on memory.

For example: Running a web browser, such as Chrome inside an enclave can prevent the privilege malware from having the access to all information. Therefore, if a distributed application is inside of enclave, the other process can not access it directly, in other word, it prevent the attacks (like hook the process).

Question 9

Please do a literature survey on Software-Defined Networks(SDN) and its implications/changes to the implementation of current popular distributed applications or systems? Advantages or new issues brought by SDN? It doesnt have to be comprehensive. A case study is fine.

Answer:
Software-Defined Networks(SDN) is to provide an enabling development of software that can control the connectivity provided by a set of network resources and the flow of network traffic through them, along with possible inspection and modification of traffic that may be performed in the network. It is basically a new way to manging the networks which separates network control from the network packing forwarding

The advantage of SDN in distributed application are: it reduces the cost of hardware, it is the centrally control, therefore it is suit for all current network management system. It improves the management and planning for a large scale system.

For example, OpenFlow by IBM use the SDN to manage their network services in LaaS. As well as many other companies, such as Huawei, Cisco, Dell Force10, Extreme Networks, IBM, Juniper Networks.

The drawback is that, the small organization get less benefit than large companies. Currently, SDN is used in the major telecom providers, big data centers and ISP because the benefits we discuses above. The small organization do not get benefit as same as the large companies.

Also the security concerns about SDN make it hard to deploy by small companies, it includes what if the control panel is under the Man-in-Middle attacks.