2nd Partial, Theory (TSR)

This exam consists of 40 multiple choice questions. In every case only one of the answers is correct. Answers must be provided in a separate template. All questions have the same value. If correctly answered, they contribute 0.25 points to the final grade. If incorrectly answered, the contribution is negative, equivalent to 1/5th of the correct value; i.e., -0.05 points. So, think carefully your answers.

Length for this part of the exam: 2 hours.

1. The Byzantine failure model...

A	...shouldn't be assumed for developing a real distributed service, since an actual set of computers cannot have that behaviour.
B	...assumes that processes may have any arbitrary behaviour.
C	...doesn't make sense nowadays. As its name suggests, it represents the behaviour of ancient computers, instead of that of modern ones.
D	...assumes that processes may only fail by halting and process failures may be detected by other processes.
E	All the above.
F	None of the above.

2. When we design an algorithm assuming a *stop* failure model...

A	...the resulting algorithm is usually simple since we assume that processes behave according to their specifications until they fail.
B	...we may find problems to implement such algorithm, since operating systems and middleware cannot guarantee a perfect behaviour for processes.
C	...we assume that processes only fail by halting and such failures can be detected by correct processes.
D	...we assume that communication channels behave correctly.
E	All the above.
F	None of the above.

3. There is a network partition failure when...

A	...a process is halted.
B	...a process has an arbitrary (i.e., outside its specifications) behaviour.
C	...a database is fragmented and distributed among multiple computers, but in an incorrect way (e.g., losing some rows in several tables).
D	...the CAP theorem is not respected.
E	All the above.
F	None of the above.

4. In the "primary partition" model:

A	Minor subgroups (i.e., those with less than a half of the system nodes) should be stopped.
B	All existing network channels behave as expected.
C	We are applying the CAP theorem, sacrificing partition tolerance.
D	All node subgroups may go on.
E	All the above.
F	None of the above.

5. Safety is...

A	...a qualitative attribute of dependability.
B	...the probability S(t) that a distributed system is restored at time t if it had failed at time t'=0.
C	...a failure model.
D	...one of the aspects being considered in the CAP theorem.
E	All the above.
F	None of the above.

6. Replication improves service performance when...

A	...we use a ROWA (read one, write all) protocol and most operations only imply read accesses.
B	...all the operations imply write accesses.
C	...the replicas are continuously recovering due to process failures.
D	...a passive replication model is used, network connectivity is lost and state updates cannot be propagated to backup replicas.
E	All the above.
F	None of the above.

7. In the passive replication model:

A	Multiple replicas may receive and directly process any client request.
B	All replicas play the same role.
C	In order to implement it, we cannot assume the arbitrary failure model.
D	In order to implement it, we cannot assume the stop failure model.
E	All the above.
F	None of the above.

8. About data-centric consistency models:

A	Causal is stricter than cache.
B	Processor is stricter than causal.
C	Cache is stricter than FIFO.
D	Sequential is stricter than cache.
E	All the above.
F	None of the above.

9. Coupling measures...

A	...the degree of dependency between the modules of an application.
B	...the reliability of an application.
C	...service continuity.
D	...whether each one of the dimensions considered in the CAP theorem is guaranteed.
E	All the above.
F	None of the above.

10. Weak cohesion isn't convenient because...

A	...always leads to faults, errors and failures.
B	...implies availability loss.
C	...it is unclear which is the functionality of each operation. This prevents modules from being reused in other applications.
D	...ensures strong consistency among service replicas.
E	All the above.
F	None of the above.

11. In a distributed service with weak coupling:

A	Request messages are generally small.
B	The amount of inter-component interactions is minimised.
C	There is a high degree of locality in data accesses.
D	Each operation only requires a few arguments.
E	All the above.
F	None of the above.

12. NoSQL datastores...

A	...ensure data consistency using ACID transactions.
B	...are usually more scalable than relational database management systems.
C	...do not ensure data persistence.
D	...have a complex query language based on the "join" operator.
E	All the above.
F	None of the above.

13. Key-value datastores…

A	...are examples of relational database management systems.
B	...use a schema based on objects with a variable number of attributes.
C	...examples are MongoDB and SimpleDB.
D	...examples are Cassandra and PNUTs.
E	All the above.
F	None of the above.

14. About extensible record datastores…

A	They use schemas based on tables with a variable number of columns.
B	They use sharding for improving their scalability.
C	One example is Bigtable.
D	One example is Cassandra.
E	All the above.
F	None of the above.

15. About the CAP theorem…

A	It relates consistency, availability and partition-tolerance.
B	Its result only makes sense in synchronous distributed systems.
C	It states that strong consistency and high availability cannot be assured simultaneously.
D	It relates data consistency, atomicity and persistency.
E	All the above.
F	None of the above.

16. About the CAP theorem consequences…

A	To develop a highly available and partition-tolerant service, we need to use eventual consistency.
B	To develop a strongly consistent (e.g., sequential) and highly available service we shouldn't tolerate network partitions.
C	Eventual consistency is almost mandatory for scalable services, since they should be highly available and should overcome network partitions.
D	The "primary partition" model is assumed in order to sacrifice availability, manage network partitions and assure strong consistency.
E	All the above.
F	None of the above.

17. The three dimensions of scalability are...

A	...consistency, availability and partition-tolerance.
B	...reliability, security and safety.
C	...hardware, firmware and software.
D	...user interface, business logic and persistent data.
E	All the above.
F	None of the above.

18. Vertical scalability consists in...

A	...adapting the computing capacity to the current workload.
B	...ensuring service continuity while the computer is upgraded.
C	...increasing the amount of nodes where a service is running.
D	...improving the computing capacity of a single node.
E	All the above.
F	None of the above.

19. Horizontal scalability consists in...

A	...adapting the computing capacity to the current workload.
B	...ensuring service safety while the computer is upgraded.
C	...increasing the amount of nodes where a service is running.
D	...improving the computing capacity of a single node.
E	All the above.
F	None of the above.

20. Four complementary mechanisms for achieving scalability on size are...

A	...reliability, availability, maintainability and safety.
B	...task distribution, data distribution, replication and caching.
C	...strict consistency, sharding, active replication and partition tolerance.
D	...elasticity, cloud computing, grid computing and P2P computing.
E	All the above.
F	None of the above.

21. Properties of decentralised algorithms:

A	Failure of one process ruins the algorithm.
B	Processes take decisions based on local information.
C	Processes assume that a global clock exists.
D	One process has complete information about the system state.
E	All the above.
F	None of the above.

22. ***Sharding*** **enhances scalability because…**

A	It is a mechanism based on data distribution.
B	It is a mechanism that provides load balancing.
C	It increases the concurrency degree; i.e., the resulting service is able to process a large amount of concurrent requests.
D	When it is appropriately designed, it doesn't demand any synchronisation step.
E	All the above.
F	None of the above.

23. A service is elastic when…

A	...it is reliable and highly available.
B	...it is dependable and uses a fast consistency model.
C	...it is scalable and with dynamic and autonomous adaptability.
D	...it is fault-tolerant and secure.
E	All the above.
F	None of the above.

24. In order to implement an elastic service, we need…

A	A monitoring system for the current workload.
B	A reactive system that automatizes service reconfiguration, taking scale-out and scale-in decisions.
C	A reactive system that considers the service level agreement.
D	A monitoring system for the current throughput.
E	All the above.
F	None of the above.

25. The main goals of security are...

A	...to ensure data consistency and persistence.
B	...secrecy, integrity, availability and accountability.
C	...safety, reliability, availability and maintainability.
D	...transparency, service continuity, performance and efficiency.
E	All the above.
F	None of the above.

26. The goal of a security policy is:

A	To ensure the correctness of a security system.
B	To implement a security system.
C	To specify a security system.
D	To measure the dependability of a system.
E	All the above.
F	None of the above.

27. About security mechanisms:

A	They are techniques and tools needed for implementing security.
B	There are three main classes: physical, authentication-related and authorisation-related (i.e., related with access control).
C	An example is the use of passwords.
D	An example is the file permission bits in UNIX file-systems.
E	All the above.
F	None of the above.

28. A security threat is:

A	A weakness in devices, protocols, programmes or policies in a system.
B	The probability T(t) that a system performs its functions at time t if it has been functioning correctly since time t'=0.
C	A model that specifies which divergences are allowed in the replicas of a given data element.
D	A set of rules that specifies which actions are authorised to the principals in a given system.
E	All the above.
F	None of the above.

29. Examples of security policy vulnerabilities:

A	Denial of service.
B	Man in the middle.
C	SYN floods.
D	Lack of disaster recovery plans.
E	All the above.
F	None of the above.

30. Examples of configuration vulnerabilities:

A	Unstructured threats.
B	To allow fragile passwords.
C	Packet sniffers.
D	Phishing.
E	All the above.
F	None of the above.

31. About mechanisms in cryptographic protocols:

A	A MAC ensures non-repudiation.
B	A certificate is a mechanism for providing accountability.
C	One-way functions are used in both MAC and certificates.
D	Symmetric cypher needs two complementary and distinct keys, one for encrypting and another for decrypting.
E	All the above.
F	None of the above.

32. Cryptographic protocols. Key distribution:

A	With symmetric cypher, we only need to distribute the private key.
B	With asymmetric cypher, we only need to distribute the public key.
C	In symmetric cypher, information leakage is not a problem.
D	In asymmetric cypher, we need secret channels to distribute keys.
E	All the above.
F	None of the above.

33. In the basic (synchronous) request/reply pattern:

A	Client requests may be delivered in non-FIFO order to the server.
B	The client can send another request before obtaining the reply for the current one.
C	If the server crashes before replying a given request to the client, the client blocks forever.
D	This pattern is implemented using PUSH and PULL ZeroMQ sockets.
E	All the above.
F	None of the above.

34. In order to deploy the basic request/reply pattern, considering ZeroMQ sockets...:

A	Clients bind their addresses and servers connect to them.
B	Servers bind their addresses and clients connect to them.
C	Both clients and servers need a single socket. Both client and servers bind their addresses and may also connect to other sockets.
D	No socket is needed to implement this architectural pattern.
E	All the above.
F	None of the above.

35. The basic PUSH-PULL architectural pattern…

A	...is a bidirectional communication pattern.
B	...is a synchronous communication pattern.
C	...is a multicast communication pattern.
D	...is an asynchronous communication pattern.
E	All the above.
F	None of the above.

36. In the advanced client/server architectural pattern with multiple clients and multiple servers interconnected by an intermediate queue…

A	Each server instance is a single point of failure for that service.
B	The intermediate queue is stable. In its simplest configuration, its sockets are bound.
C	The intermediate queue uses PUSH-PULL sockets.
D	Clients use SUB sockets.
E	All the above.
F	None of the above.

37. Heart-beats are used in some advanced client-server architectures in order to…

A	...detect client failures.
B	...monitor the current workload.
C	...improve the scalability of servers.
D	...implement cryptographic protocols.
E	All the above.
F	None of the above.

38. Retries are used in some advanced client-server architectures in order to...

A	...detect server failures.
B	...implement a load balancing mechanism.
C	...improve the scalability of servers.
D	...detect client failures, combining them with timeouts.
E	All the above.
F	None of the above.

39. In order to implement a mechanism for recovering in case of a non-idempotent request failure, we need:

A	To identify clearly each request message, with an <id-sender, id-request> pair.
B	Before serving each request, the server should look for that request in its “reply store”.
C	If a request is found in the “reply store”, the reply message is taken from there and sent to the client.
D	After serving each request, the server copies the reply message to a local “reply store”.
E	All the above.
F	None of the above.

40. In the advanced client/server architectural patterns from Unit 9, servers are replicated in the following way…

A	The active replication model is used.
B	All service operations are idempotent.
C	The passive replication model is used.
D	Both primary and back-up replicas use a heart-beat module to detect client failures.
E	All the above.
F	None of the above.