DISTRIBUTED SYSTEMS
CHAPTER 1&2

1. In distributed system each processor has its own
a) local memory
b) clock
c) both (a) and (b)
d) none of the mentioned
View Answer

Answer:c

2. If one site fails in distributed system
a) the remaining sites can continue operating
b) all the sites will stop working
c) directly connected sites will stop working
d) none of the mentioned
View Answer

Answer:a

In distributed systems, link and site failure is detected by
a) polling
b) handshaking
c) token passing
d) none of the mentioned
View Answer

Answer:b

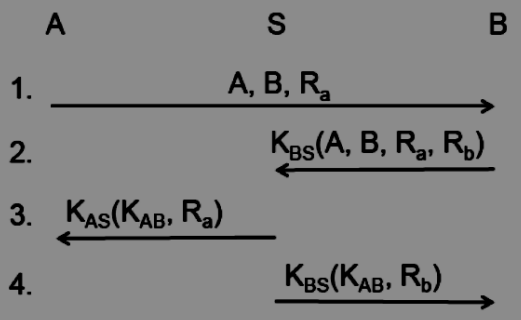
The capability of a system to adapt the increased service load is called
a) scalability
b) tolerance
c) capacity
d) none of the mentioned
View Answer

Answer:a

True False

(12 points) The following figure illustrates a protocol between two agents A and B, and a server S. The intent is to get the server to generate a shared session key K_{AB}, and to also enable A and B to make sure they are communicating with each other.

Each agent shares a private key with the server S: A has K_{AS}, and B has K_{BS}. Values R_a and R_b are randomly generated "nonces" (number-used-once). The notation $K(M_1, M_2, \ldots, M_n)$ means to generate a message containing an encrypted version of the sequence $M_1, M_2, \ldots, M_n$ using key K.



Assume the following:

- Initially, only A and S know K_{AS}, and only B and S know K_{BS}.
- The true server S is not malicious, but there could be an imposter S′ trying to pose as S.
- There could be an imposter A′ or B′ trying to pose as A or B.
- Imposters can intercept any traffic, replay old messages, or inject new ones.
- The encryption is secure, and the encrypted form of the sequence does not reveal any information about the encrypted form of the individual elements. For example, knowing $K(M_1, M_2)$ does not reveal any information about $K(M_1)$ or $K(M_2)$.
- We will say that a message is *freshly generated* if it must have been created some time after the initial message in the protocol.

For each of the following statements, state whether it is true or false. Give a brief (one or two sentences should suffice) justification for your answer.

Solution: This protocol has a vulnerability that was not recognized at the time the exam was created. An imposter B′ could intercept message 1 and send the message $K_{B'S}(A, B', R_a, R_b)$ to S. S would generate a session key $K_{AB'}$ and send a message $K_{AS}(K_{AB'}, R_a)$ to A. Since message 3 does not identify the involved parties, A would not realize that it had created a session with B′ rather than B.

In the below answer key, we give both the intended answer and the correct answer, in terms of this vulnerability. We accepted either version but required the answers be consistent and properly explained.

Note: this vulnerability could be avoided by including the identities of A and B in messages 3 and 4.

(a) S can be certain that message 2 was freshly generated by B.

Solution: False. This could be a replay of an old message, since there is no guarantee that R_a is fresh.

(b) A can be certain that message 3 was freshly generated by S.

Solution: True. Only someone who knew K_{AS} could have generated $K_{AS}(R_a)$

(c) B can be certain that message 4 was freshly generated by S.

Solution: True. Only someone who knew K_{BS} could have generated $K_{BS}(R_b)$

(d) Upon completion of the protocol, A can be certain that it has established a session with B.

Solution: Intended: True. Since A knows that R_a is fresh, it can be certain that S must have received message 2 from B.
Corrected: False. As noted above, the session could be with an imposter B′.

(e) Upon completion of the protocol, B can be certain that it has established a session with A.

Solution: False. A has not established its identity with either B or S.

(f) Upon completion of the protocol, no one other than A, B, or S can know the value of K_{AB}.

A:1 1p. What is meant by access transparency?

A remote resources are accessed using location independent names

- B local and remote resources are accessed using the same operations

C a replicated resource is accessed exactly as if it was a single object

D a resource will handle all requests equally independent of location of client

A:2 1p. What is meant by location transparency?

- A remote resources are accessed using location independent names

B local and remote resources are access using the same operation

C a replicated resources is accessed exactly as if it was a single object

D a resource will handle all request equal independent of location of client

A:3 1p. What is meant by concurrency transparency?

A threads are allowed to access shared data structures

- B processes can access resources without interfering with each other

C a replicated resources is accessed exactly as if it was a single object

D new nodes can be added to a system without changing the application

A:4 1p. What is meant by failure transparency?

- A failures are concealed for the users of a resource

B resource errors will raise exception that can be handled by the user

C resources can fail but only by crashing

D a robust system where resources will not fail

A:5 1p. What is meant by replication transparency?

A processes have knowledge of replication scheme and can take advantage of it

- B users of a resource access it as if it was not replicated

C data is immutable and can be serialized on disk

D replies to queries are copied and logged to avoid dirty reads

A:6 1p. What is significant for a client server architecture?

- A the client is the active part

B servers have more execution power

C several clients but only one server

D the server is the active part

A:7 1p. What would we call a system where one node is always reacting on requests and other nodes only communicate with this node?

A an asynchronous system

- B a client server system

C a peer-to-peer system
D a synchronous system
What is the definition of total-order multicast? 16
A messages are delivered in FIFO order
B messages are delivered in real time order
C messages are delivered in happen-before order

- D messages are delivered in the same sequence

ANSWER THE FOLLOWING:

- Explain two benefits of middleware to distributed system programmers, providing an example

for each benefit.
Solution: Some benefits are:
• Middleware can provide high-level abstractions that make it easier to develop distributed systems.
These abstractions hide some of the details of the implementation of the system. For example, RPC hides marshaling and communication code behind a procedural interface to remote procedures.
• Middleware isolates the programmer from the operating system.
Programs can be written to the middleware layer and can be (more easily) ported to other machines that support the same middleware (i.e., CORBA implementations are available on a variety of machines).
• Middleware can provide some forms of transparency to the programmer automatically. For
example, middleware can handle the data representation problem, converting data in messages
so they are appropriate for the architecture on which the receiving process is running.

- What are three advantages of client-server systems? What are three advantages of peer-to-peer systems?

Solution: The advantages of client-server systems are the following:
1
1. More efficient division of labor between the client machines and the servers.
2. Horizontal and vertical scaling of resources are possible.
3. Better price/performance on client machines possible since they don’t need to be as powerful.

4. Ability to use familiar tools on client machines since users can use their own machines as clients.
5. Clients can access remote data and resources.
6. Overall better system price/performance.
The advantages of peer-to-peer systems are the following:
1. Uniform functionality among machines since there is no separation of clients and servers.
2. Better scalability since servers would not be bottlenecks.
3. Less initial expense, since there is no need for a dedicated server.
4. Possibly better system availability since there are no centralized servers.

TRUE / FALSE
A "broadcast network" is one which uses radio-frequency transmission to send data from one party to another.
EXPLAIN: *A "broadcast network" is one in which multiple receivers can receive a message at the same time from a single sender.*

TRUE / FALSE
A Remote Procedure Call (RPC) can be used to call a procedure in another process on the same machine.
EXPLAIN: *Just make the client and server addresses to be the same. Location transparency is a fundamental aspect of RPC.*