⑤ Denial of Service: flooding a channel or other resource with msgs to denial other's access

② Masquerading: sending or receiving msg using ID of another principal without authority

③ Message Tampering: Intercepting msgs & altering their content

④ Replaying: storing Intercepted msgs & send them at later date

Obtained score
14

Question 1:

Explain why are distributed systems vulnerable to security attacks? List and define the main types of attack faced by distributed systems. Give an example of each type of attack.

[14 marks]

Vulnerable: ① DSs are open to external access
② offer exposed interface
③ Internet is insecure

Obtained score

Question 2:

Types of Attack: ① Eavesdropping = obtaining copies of message without authority

Name 2 techniques to aid scalability of distributed systems. Provide an example for each.

[10 marks]

Obtained score

Question 3:

Name and describe 3 types of possible transparency in distributed system.

[6 marks]

Obtained score
10

Question 4:

With a P2P file sharing, what are the advantages for a query flooding system like Gnutella over a centralized query system like Napster?

[10 marks]

① No Single Point Failure : Gnutella continue working if nodes are down,

② Better Scalability : Peers can store more data; will not cause network traffic to the "central" node.

③ Dynamic ~~Adaptton~~ adaptation : Networks are Self-organized

Obtained score
15

Question 5:

a) What is *cryptography* and what are the main *3 uses of cryptography* presented in this course? Briefly present each use (of the 3 main uses of cryptography) and provide a relevant example for each of these uses.

Cryptography = the study of mathematical techniques related to aspect of info security.

[7 marks]

b) What are the main differences between Symmetric and Asymmetric Encryption algorithms? Briefly explain each of these differences.

[8 marks]

[Total 15 marks]

a) Uses: ① ~~Symmetric keys~~ Security & Integrity = Ensuring the safety & correctness of info
② ~~Asymmetric keys~~ Authorization = Control access permission.
③ ~~Hashed algorithms~~ Authentication = Validate ID

b) Symmetric = Use single key / Old / keys must be delivered securely
Asymmetric = uses a pair of public key & private key / relative new / Takes more time

Obtained score
10

Question 6:

Name two algorithms that are used to synchronize physical time in a distributed system?
Discuss and explain how each of the two algorithms works.

[10 marks]

Question 6: ① Chistian's Algorithms: $T_{CLIENT} = T_{SERVER} + (T_1 - T_0)/2$

② Berkeley Algorithms: Master node calculates the AVG time difference between all the clocks time. This AVG difference is added to master's clock & broadcast over network

Obtained score

Question 7:

When using a *cache* in a distributed system, what policies can be used to decide when a cache should be updated?

[5 marks]

Obtained score
10

Question 8:

In a peer-to-peer system, what is a *routing overlay*? Describe how the Pastry peer-to-peer middleware implements routing.

[10 marks]

Question 8: RO: Is the routing solution for locating resources In Middleware System
It's resposible for: ① Direct request to the node with a replica inside

Obtained score
10

Question 9:

② Greet GUID ③ Announcing existence of new resource ④ remove of disappered resource
⑤ managing nodes in system   Pastry: Check Msg ID with NodeID → Leaf Set
→ Routing table with longer prefix → Forward to numerically closer.

In a distributed system, what is an *Election Algorithm* and what it is used for? Briefly present the two election algorithms considered in this course.

[10 marks]

Election Algorithms choose process from a group of processes to act as coordinator / used for: Determines where a new copy of the coordinator should be restarted

Obtained score
10

Question 10:

Two Algs = Ring Algorithms: applies to systems organized as a ring. If Any process failure, It constructs an election msg

What is *mutual exclusion*? Discuss how mutual exclusion may be implemented in distributed systems. Your answer should describe the three approaches discussed in this course, namely: *centralised*, *distributed*, and *token ring*.

[10 marks]

Question 10:

Centralised: Good: Fair, no process starvation
Ez to impl
Bad: Single point of failure
coordinator is the bottleneck

Distributed = Good: No single point of failure
Bad: Multiple point of failure
A "crash" is interpreted as a denial of entry to the critical space. / Slow.

Token Ring: Good = Fair
Bad = Token could be LOST
Process failure cause problem
Every process is required to maintain the current logical Ring in Mem

with its process ID & send it to its successor. If successer down. it skip over it & sends the msg to the next party. This process is repeated until a running process located.
Bandwidth: $3N-1$
Turnaround time: $3N-1$

Bully Algorithm: