**Northeastern University – Silicon Valley**

CS 6650 Scalable Dist Systems

**Homework #5** [100 points]

**Name: Nisarg Patel**

**Email:** [**patel.nisargs@northeastern.edu**](mailto:patel.nisargs@northeastern.edu)

***INSTRUCTIONS: Please provide clear explanations in your own sentences, directly answering the question, demonstrating your understanding of the question and its solution, in depth, with sufficient detail. Submit your solutions [PDF preferred].* Include your full name*. Do not email the solutions.***

1. Security Engineering Ch. 11 please answer

11.2 [5 points]

**Ans:**

A conventional email communication includes a sender, a receiver and a channel over which email is sent. The conventional email is vulnerable to different ways in which the channel is being misused:  
1) Eavesdropping: The email is not encrypted before sending. It can be protected by using an encryption algorithm, thus encrypting the email during sending and decrypting during receiving.

2) Masquerading: The sender(or receiver) authentication is missing. It can be protected by digitally signing the email before sending it.

3) Message Tempering: A secure connection is not established for the channel, thus resulting in man-in-the-middle attacks. The proof of secure channel can be established by both sender and receiver sending a digitally signed and encrypted message through the channel before sending the email.

4) Replaying: This type of attack can happen with secure channel if the email message is not timestamped. To protect from this, timestamps can be added to the email message.

5) Denial of Service: It can happen if the channel is open for multiple connections, and one of the senders tries to block the channel. It can be prevented by putting a limit on number of emails that can be sent by a sender in a time period in the channel.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

11.3 [10 points]

**Ans:**

Some of the defences against man-in-the-middle attacks during initial exchanges of public keys are:

1. A third-party key-distribution service can be used to get a public key certificate. This certificate can than be entrusted with security and public keys of both parties can be read from this certificate after ensuring the validity of the certificate.
2. A secondary secure channel like TLS can be established that shares only the public key. The further communication can be encrypted and sent on insecure channels.
3. Another way of sharing public keys can be by using CD-ROM or other hardware devices that stores public keys and certificates which are accessible to only the corresponding parties.
4. The service’s domain name can be included in it’s public-key certificates so that clients can only acknowledge the service from the corresponding IP address only.
5. A non-digital way of communication can be used for initial exchanges of public keys. Some of the methods include verbal communication of the key, or sharing keys handwritten by both parties.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. (please ignore the last sentence – parallel processor enhancement part) [10 points]

**Ans:**

We are assuming the values from figure 11.13, Crypto++ 2.1 GHz Pentium 4 for finding the encryption times.

**56-bit DES:**

**Encryption time per key:**

Performance =

Thus, time to encrypt 8 bytes = =

**Inner loop time per key:**

Instructions per key = 10 /s

Computer speed = 2000 Million Instructions / s

Thus, time to compute inner loop per key = 10 / (2000 x 10^6) = 10/(2 x 10^9) = 5 x 10^-9 sec

**Average Time required to crack:**

Key length for DES = 56

Total possible keys = 2^56

Average keys to process before cracking = (2^56)/2 = 2^55

Total time per key = 3.75 x 10^-7 + 5 x 10^-9 = 3.8 x 10^-7 sec

Thus, average time required to crack = 2^55 x (3.8x 10^-7) = 1.37 x 10^10 sec ≈ 434 years

It will take approx. **434 years** to crack the 56 bit DES key using 2000 MIPS

**128-bit IDEA:**

**Encryption time per key:**

Performance = 18.963 Mbytes/s

Thus, time to encrypt 8 bytes = 8/(18.963 x 10^6) = 4.22 x 10^-7 sec

**Inner loop time per key:**

Instructions per key = 10 /s

Computer speed = 2000 Million Instructions / s

Thus, time to compute inner loop per key = 10 / (2000 x 10^6) = 10/(2 x 10^9) = 5 x 10^-9 sec

**Average Time required to crack:**

Key length for DES = 128

Total possible keys = 2^128

Average keys to process before cracking = (2^128)/2 = 2^127

Total time per key = 4.22 x 10^-7 + 5 x 10^-9 = 4.27 x 10^-7 sec

Thus, average time required to crack = 2^127 x (4.27 x 10^-7) = 7.26 x 10^31 sec ≈ 2.3 x 10^24 years

It will take approx.  **years** to crack the 128-bit IDEA key using 2000 MIPS.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Multimedia Apps Ch. 20 please answer

20.2 [5 points]

**Ans: (Sol 15.2)**

The Internet does not currently offer any resource reservation or quality of service

management facilities. How do the existing Internet-based audio and video streaming

applications achieve acceptable quality? What limitations do the solutions they adopt

place on multimedia applications? *pages 884, 893, 899*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

20.3 [10 points]

**Ans: (Sol 15.3)**

Explain the distinctions between the three forms of synchronization (synchronous

distributed state, media synchronization and external synchronization) that may be

required in distributed multimedia applications. Suggest mechanisms by which each of

them could be achieved, for example in a video conferencing application. *page 885*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

20.4 [10 points]

**Ans: (Sol 15.4)**

Outline the design of a QoS manager to enable desktop computers connected by an

ATM network to support several concurrent multimedia applications. Define an API for

your QoS manager, giving the main operations with their parameters and results.

*pages 889–891*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Ch 18 Replication [25 points]
2. 18.1

**Ans: (Sol 14.1)**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Study only pages 2 to 7 of the IBM Redbook

### [IBM High Availability Solution for IBM FileNet P8 Systems](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjYu6Ky0an7AhUHm2oFHUrxD6M4HhAWegQIIxAB&url=https%3A%2F%2Fwww.redbooks.ibm.com%2Fredbooks%2Fpdfs%2Fsg247700.pdf&usg=AOvVaw2smGgtV-zOXwUdKFnZMCxD)

Define Availability.

For a typical web app cluster (Web server, App server, Db server) with Active-Active redundancy using a total of 6 servers (2 replicas of the same web cluster), explain how Availability calculations are made and how HA can be achieved. Show your calculations.

**Ans:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Ch 19 Mobile computing [25 points]
2. 19.1

**Ans:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Consider the Uber car hiring platform. In this context, what is adaptation? How is it used in the overall design and what problems/requirements is it addressing?

**Ans:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_