ECLT5820 Distributed and Mobile Systems

Assignment 1 (Topics 1-4)

Due – 11:59pm, 14th Oct, 2020 (Wednesday)

Note: Please send a pdf file to eclt5820@cse.cuhk.edu.hk with email title and file name "ECLT5820 Asg#1, Your name, Your student ID".

Q1 (**15 points**) Hadoop Distributed File System (HDFS) has been employed by various distributed applications, such as Apache Spark. HDFS is a distributed file system that provides scalable and reliable data storage, and it was designed to span large clusters of commodity servers. Please visit https://en.wikipedia.org/wiki/Apache_Hadoop first if you have not heard about HDFS. We will discuss this technique in Cloud Computing lecture in more detail.

Compare with the traditional native apps, please justify the key differences of HDFS from the following perspectives:

1) Heterogeneity
2) Openness
3) Security
4) Scalability
5) Failure Handling
6) Concurrency

Q2 (**15 points**) List the three main software components that may fail when a client process invokes an operation in a server process, giving an example of a failure in each case. To what extent are these failures independent of one another? Suggest how the components can be made to tolerate one another's failures.

Q3 (**15 points**) The Chinese University of Hong Kong employs Blackboard platform to help students organize their courses. Please explain your choice about whether we should use TCP or UDP protocol to implement the following application-level usage cases:

1) Type the address to access Blackboard, which would use Domain Name System (DSN).
2) Download course assignments or upload your answers.
3) Browse course contents.
4) Watch lecture video.
5) Is UDP more reliable than TCP? Please justify your answer with details.

Q4 (**15 points**) The development of electronic mail (email) was the first Internet killer application, driving Internet use as the light bulb drove the acceptance of electricity. Conventional user-level email clients typically use SMTP protocol for sending messages to a mail server for relaying. For retrieving messages, IMAP and POP3 are standard protocols. (Note: You don't need to know details of these protocols, although you can Google them.)

Describe some of the ways in which conventional email is vulnerable to eavesdropping, masquerading, tampering, replay, denial of service. Suggest methods by which email could be protected against each of these forms of attack.

Q5 (**25 points**) Consider the RSA encryption algorithm. Please write down your computation details.

1) p=5, q=17, and e=7, what is the corresponding public key and a possible private key?
2) Try to encrypt '12' with the public key and decrypt '18' with the private key.
3) If public key and private key for an RSA algorithm are the same, then there is certainly no security, but mathematically can they be the same? If so, please give an example. If not, please prove or show it.

Q6 (**15 points**) What are Naming service and Trading service? What are the differences between them? What are the pros and cons of them when comparing with each other?