Network Security
Assignment 04
(Kerbros, X.509 and SMIME)

Distribution date: Apr 22, 2011 Due date: April 30, 2011, at 23:59 pm.

Note Carefully:

- Send your assignment by email at asimrasheed@mcs.edu.pk only. Submission to any other address is not accepted.
- There is a 25% penalty on late assignments, up to half an hour. More than half an hour late assignments will NOT be accepted, what so ever is the reason.
- Total points for this assignment are 50, which will be scaled down as per plan.
- Important for Email Submission:
- The subject field of your email must be "Assignxx_full_name_Regno". For example, Assign04_Asim_Rasheed_123456.
- The name of the solution document file must also be AssignxxfullnameRegno.pdf. For example, Assign04Asim_Rasheed_123456.pdf.
- Only.pdf formats are accepted.
- At most ONE attachment will be accepted. Multiple attachments will not be entertained.
- You MUST NOT send your assignment to the course mailing list: it will NOT be accepted, and you may get discredit.
- Submission time is NOT the time when you email your assignment; rather it is the time BEFORE which we must receive your email.
- We encourage you to send your assignment two hour before the deadline ends.

Important for Cheating Cases:
This is an individual assignment. Cheating is strictly prohibited. Students found involved in the cheating/copying (irrespective of doing or allowing) will be marked simply as ZERO.

Important for all questions: Use your own wording to explain the answers. Just copy / paste / edit from the research paper will not receive the credit.

Q No 01: (6 Marks)
Why we need Kerberos architecture. Do you feel some other easy and more efficient ways to do authentication as proposed by Kerbros?

Read the paper "Dos and Don'ts of Client Authentication on the Web" by Kevin Fu, Emil Sit, Kendra Smith, Nick Feamster and answer the following questions.

Q No 02: (6 Marks)
What is brief client authentication scheme proposal?

Q No 03: (4+4 = 8 Marks)

Paper claims more secure scheme against forgeries by the interrogative adversary and in conjunction with SSL, and active adversary.
1. Explain the proof and your comments on justification?
2. Explain interrogative adversaries and active adversaries?

Q No 04: Encrypting the decrypted text using S-MIME (30 Marks)
You will generate a PKCS12 file using Openssl command line executable file. You will use the certificate with your outlook express (or any other supporting mail client) to sign and encrypt the text which is in "decrypted_text.txt" file with your name and reg# written in it. You can find free POP/SMTP services from the following link
• http://www.iopus.com/guides/bestpopsmtp.htm
you will send this encrypted & signed message (separately) to asimrasheed@mcs.edu.pk

Restrictions
• You can only use Openssl and Gnu PG (GPG).
Linux is not required you can setup on your windows machine.

Deliverables
Your submitted project zip file should include
• decryptedtext.txt
• decryptedtext.txt.gpg or decryptedtext.txt.asc
• ID file
• Your generated PKCS12 file (certificate)

Your encrypted & signed message on the above mentioned email.