Monash University
Faculty of Information Technology
FIT3031 Information and network security

Class Test

Instructions to Candidates:

1. **First complete this section**

*You must complete this section*ß

STUDENT ID:____

STUDENT NAME : ____

□ TUTOR NAME : ANIT

□ TUTOR NAME : LELE SHA

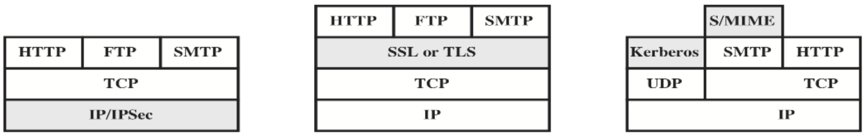
□ TUTOR NAME : ABDUL MALIK

2. The coverage material from LN01 to LN08 (inclusive of LN08 IP Security).
3. There are 2 parts to the test.
4. Answer all questions in the space provided in each part.
5. Marks are indicated at the beginning of each question.
6. This class test is worth 20 % of UNIT marks.
7. The duration of this class test is 60 minutes.
8. Total marks = 70.
9. **Return the question paper intact.**

Part 2: Answer the following questions in the space provided:

(17 +12 + 11 = 40 marks)

1. **Question-1. (9+4 +4) = 17 marks)**
   a. S/MIME, Kerberos, SSL/TLS, IPsec, HTTPS and PGP are all ways to secure data exchange. Using an appropriate and well-labelled diagram, for each technique, indicate how it can be placed with respect to the TCP/IP layered model. **[9 marks]**



(a) Network Level (b) Transport Level (c) Application Level

Figure 5.1 Relative Location of Security Facilities in the TCP/IP Protocol Stack

Ans: The advantage of using **IPSec** (Figure 5.1a) is that it is transparent to end users and applications and provides a general-purpose solution. Further, IPSec includes a filtering capability so that only selected traffic need incur the overhead of IPSec processing. The advantage of using **SSL** is that it makes use of the reliability and flow control mechanisms of TCP. The advantage of **application-specific security services** (Figure 5.1c) is that the service can be tailored to the specific needs of a given application.

b. List and describe both the basic approaches to bundling SAs? **[4 marks]**

Answer:
Transport adjacency: Refers to applying more than one security protocol to the same IP packet, without invoking tunneling. This approach to combining AH and ESP allows for only one level of combination; further nesting yields no added benefit since the processing is performed at one IPSec instance: the (ultimate) destination.

Iterated tunneling: Refers to the application of multiple layers of security protocols affected through IP tunneling. This approach allows for multiple levels of nesting, since each tunnel can originate or terminate at a different IPSec site along the path.

c. List **three** advantages and **one** limitation of CTR mode of operation? **[4 Marks]**

1. efficiency
2. can do parallel encryptions in h/w or s/w
3. can pre-process in advance of need
4. good for bursty high speed links
5. random access to encrypted data blocks
6. provable security (good as other modes)

1. but must ensure never reuse counter values, otherwise could break (cf OFB)

(1 MARKS FOR EACH POINT)

2. **Question-2. (4 + 4 +4 = 12 marks)**

a. Explain how PGP achieves public key management. **[4 marks]**

Rather than relying on certification authorities, in PGP every user is a CA. [1 mark]

A user can sign keys for users they know directly. [1 mark]

They form a “web of trust” and can trust keys others have signed if they have a chain of signatures to them. [2 mark]

b. When a Client (C) presents a service granting ticket (SGT) to a server (S) in a system that uses **Kerberos** to provide the authentication service, the client must also attach an authenticator to prove that he is the legitimate holder of the ticket. How can the server (S) verify that the authenticator belongs to the ticket's legitimate holder? **[4 marks]**

The authenticator contains the client's identity and a timestamp. These are encrypted with the session key that is known to the client and the server. [1 mark]

Therefore, a client that will create a valid authenticator has to have this session key, which has been provided by the TGS (Ticket Granting Server) to the client and the server via a ticket that has been encrypted with a key known to the TGS and the server. [1.5 mark]

Since the TGS has checked the client's legitimacy (using the ticket provided by the Authentication Server (AS)), S is sure that the client with the session key is legitimate as he is the only one who is able to create a valid authenticator with his identity. [1.5 mark]

c. You have just received an email with the digital signature of a certain Bill Thornton using **PGP**. Unfortunately, you have never exchanged a public key with any Bill Thornton. It happens that Richard Branson has signed Bill's key and John Fraser, whom you completely trust has signed Richard's key. What can you say about the validity of Bill Thornton's key?**[4 marks]**

Since Richard Branson's key is signed by John Fraser whom you trust (i.e. in the web of trust it is indicated that you already have complete trust in John Fraser who signed Richard Branson's key), [1.5 mark]

So you can consider his key as being valid. [1 mark]

However, you do not know how much trust John has in Richard Branson, therefore, you cannot validate Bill Thornton's key. [1.5 mark]

3. **Question-3. (4 + 7 = 11 marks)**

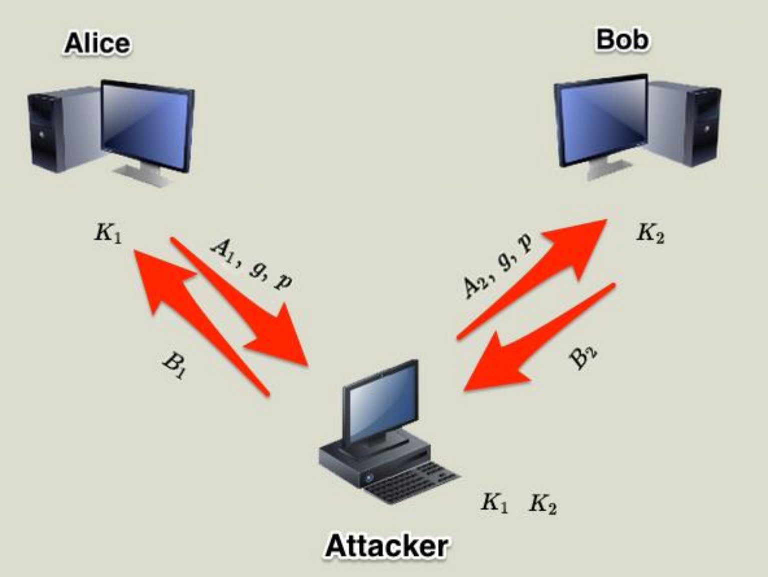
a. List **four**-design consideration for **stream** cipher? **[4 marks]**

- **some design considerations are:**
  - long period with no repetitions
  - statistically random
  - depends on large enough key
  - large linear complexity
- **properly designed, can be as secure as a block cipher with same size key**
- **but usually simpler & faster**

Example RC4

(Any 4 points x 1 Mark each)

b. Explain with the help of a suitable diagram, How a **man-in-the middle attack** is possible for Diffie-Hellman key exchange protocol? **[7 marks]**



The protocol described on the previous slide is insecure against a man-in-the-middle attack. Suppose Alice and Bob wish to exchange keys, and Darth is the adversary. The attack proceeds as follows:

1. Darth prepares for the attack by generating two random private keys X_{D1} and X_{D2} and then computing the corresponding public keys Y_{D1} and Y_{D2}
2. Alice transmits Y_A to Bob.
3. Darth intercepts Y_A and transmits Y_{D1} to Bob. Darth also calculates K2 = (Y_A)^ X_{D2} mod q
4. Bob receives Y_{D1} and calculates K1=(Y_{D1})^ X_B mod q
5. Bob transmits Y_B to Alice.
6. Darth intercepts Y_B and transmits Y_{D2} to Alice. Darth calculates K1=(Y_B)^ X_{D1} mod q
7. Alice receives Y_{D2} and calculates K2=(Y_{D2})^ X_A mod q .

At this point, Bob and Alice think that they share a secret key, but instead Bob and Darth share secret key K1 and Alice and Darth share secret key K2. All future communication between Bob and Alice is compromised in the following way:

1. Alice sends an encrypted message M: E(K2, M).
2. Darth intercepts the encrypted message and decrypts it, to recover M.
3. Darth sends Bob E(K1, M) or E(K1, M'), where M' is any message. In the first case, Darth simply wants to eavesdrop on the communication without altering it. In the second case, Darth wants to modify the message going to Bob. The key exchange protocol is vulnerable to such an attack because it does not authenticate the participants. This vulnerability can be overcome with the use of digital signatures and public- key certificates.

END OF CLASS TEST