HET317 Tutorial Week 5

Question 1

1. One of the weaknesses of the PAP authentication system is that it transmits the password in the clear. How does CHAP avoid doing this?

CHAP uses a three-way handshake. Upon completion of the PPP connection:

   a. The authenticator sends a challenge string (usually a random number) to the connecting host.

   b. The connecting host uses its password and the challenge string to generate a one way hash using a hash function such as SHA-1

   c. The authenticator (who knows the password) uses the same challenge, password and hash function to calculate the hash. If correct it sends an 'Authentication accepted' message to the host

2. What is the difference between a firewall that does 'deep-inspection' and a firewall that does 'stateful-inspection'

'Deep inspection' involves analysing the contents of the packet based on the encapsulating data. So for example if a TCP packet has a port number of 80, then its contents should conform to rules for HTTP messages (eg. GET and POST messages or http replies). State of the connection is not necessarily maintained.

'Stateful inspection' involves keeping track of the connection state. Stateful inspection is commonly used to monitor flags during the TCP three-way handshake and ensure their validity.

HET317 Tutorial Week 5

Question 2

System 1

Setting	1	2	3	4	5	6	7	8	9	10
False rejects (%)	0.5	1	1.0	2	2.5	3	4	6	9	12
False accepts (%)	4	4	3.0	3.0	2.5	2.5	2	1.5	1.5	1.0

System 2

Setting	1	2	3	4	5	6	7	8	9	10
False rejects (%)	0	0	0	0	0	3	6	10	15	20
False accepts (%)	11	8	6	4	3	3	1	0	0	0

NOTE: False reject = classifying authorised user as an imposter (Type I)

False accept = classifying imposter as an authorised user (Type II)

1. Using total error rate as a performance criterion, which is the superior system?

Minimum total error rate for System 1 is 4%. Minimum for System 2 is 3%. So system 2 is superior using this measure.

2. Using the cross-over error rate as a performance criteria, which is the superior system?

Cross over error rate for System 1 is 2.5. Cross over error rate for System 2 is 3%. System 1 is superior using this measure.

3. If a false acceptance rate of 3% is acceptable which is the preferable system?

For a false acceptance rate of 3%, System 1 has a lowest error rate of 1%. For a false acceptance rate of 3%, System 2 has a lowest error rate of 0%, so System 2 is preferable.

HET317 Tutorial Week 5

Question 3

Modulo arithmetic can be used in the generation of one-time passwords. `X mod Y` is the remainder when `X` is divided by `Y`.

1. Calculate the following:

   `5 mod 3, 10 mod 11, 15 mod 12, 2 mod 1, 5 mod 5, 10 mod 5.`

   2, 10, 3, 0, 0, 0

2. Suppose we use the function `F(X) = (5 X ) mod 9` to generate our one time passwords.

   a. Generate the first 8 passwords (including the seed value) with seed `X = 5`

   5, 7, 8, 4, 2, 1, 5, 7

   b. What will be the first password we use? The second? The third?

   We will use the passwords in the order 7, 5, 1, 2, 4, 8, (7) (ie reverse order).

3. Suppose we use the function `F(X) = (5 X) mod 3.`

   a. Generate the first 4 passwords starting with X = 5

   1,2,1,2

   b. Can you make any general observations about use of modulo arithmetic to generate passwords?

   They will eventually repeat with maximum cycle length equal to Y.

HET317 Tutorial Week 5

Question 4

Consider a simple challenge-response mechanism used for authentication. To calculate the response to the challenge, the key is added to the challenge and the hash is calculated. The hash is then returned as the response to the challenge.

The hash function is F(X) = 5 X mod 9. Each party has a shared secret key of 15. The challenge is an integer between 10 and 20.

What will be the response to a challenge of 11?

The challenge is 11. The authenticatee adds the challenge to the shared secret key giving 26. The hash of 26 using 5 X mod 9 is 5(26) mod 9 = 130 mod 9 = 4.