CSS 322 – QUIZ 5 ANSWERS

Question 1 [2 marks]

If the Authentication Header (AH) is used in IPsec when sending a File Transfer Protocol (FTP) message, select which pieces of information are authenticated (you may select more than one – you must get all correct to receive full marks):

a) Mutable fields (those that may change) in the IP header

b) The headers from Physical and Data Link/MAC layers

c) The Authentication Data field in the AH

d) The first 96-bits of the payload

e) The TCP header

f) The entire IP header

g) The FTP header

Correct answers: (e) and (g)

The structure of an IPsec packet when using Authentication Header (AH) is:

Physical | MAC | IP | AH | TCP | FTP | Data

The authentication covers the entire payload of the original IP packet, that is, TCP, FTP and Data. It also covers parts of the IP header (those parts that don't change – immutable – or a predictable) and parts of AH.

Option (a) is false because if we calculate the MAC across mutable fields (those that will change), then the authenticated data sent will be different from the authenticated data received. Therefore, the MAC (authentication) will fail, when it should pass.

Option (b) is false because IPsec doesn't provide any coverage of the lower layer (Physical, MAC/Data link) headers.

Option (c) is false because the Authentication Data field carries the actual MAC – hence it is impossible to achieve. That is, the input to the MAC function cannot include the output of the MAC function!

Option (d) is false because the scheme would be almost useless. If only 96 bits of the payload were considered, then it would be possible for the remaining bits of the payload to be changed, without the receiver detecting it.

Option (e) is true – the authentication does cover the TCP header.

Option (f) is false because of answer to option (a).

Option (g) is true – the authentication does cover the FTP (or application layer) header.

Marks: selecting (e) or (g) gave 1 mark each. Selecting an incorrect option resulted in loss of 0.5 mark. Hence, if you selected (d) and (e) you received 0.5 out of 2. If you selected (d), (e) and (g) you received 1.5 out of 2.

Question 2 [4 marks]

Multiple choice. Select the most accurate answer. Choose only one. You receive 1 mark for a correct answer. You lose 0.5 marks for an incorrect answer. 0 marks for an unanswered question.

a) If you are developing a database that stores login credentials for users (e.g. username and password), you should:

   a. Save the password as plaintext
   b. Calculate the hash of the password and save the hash value
   c. Calculate the MAC of the password using a secret key, and save the MAC
   d. Encrypt the password with AES and save the ciphertext

Correct answer: (b)

Option (a) is poor design – you should never save a password as plaintext.

Option (b) is a good design – this is the most efficient and simple of the secure approaches.

Option (c) may provide same security as (b) but is inconvenient and inefficient – you need to store and use the secret all the time.

Option (d) is also inefficient – most encryption algorithms like AES are usually more complex than hash/MAC functions. And again you need to use a secret key all the time.

b) Assume a password file storing the SHA1 hashes of passwords is on a Linux PC and the file is readable by all users of that PC. A practical approach to make the PC more secure against offline password guessing is:

   a. Automatically disable access to an account if too many incorrect attempts are made.
   b. Limit the speed at which passwords can be entered at the terminal.
   c. Automatically check the passwords when initially created by users, and reject the password if it is a "weak" password.
   d. Use the MD5 hash function instead of SHA1 hash function.

Correct answer: (c)

Options (a) and (b) are only useful for deterring online password guessing. For offline password guessing, you assume the attacker has the password file and can make as many guesses as they like at any speed on their on computer.

Option (c) is the best approach – a practical way to make offline password guessing hard is to ensure the passwords chosen are strong (so harder for an attacker to guess).

Option (d) does not help the security – in fact, one could argue that SHA1 is better than MD5.

c) Panita's X.509 certificate (which is signed by the certificate authority Pongpak) contains:

   a. Only Panita's public key (and no other keys)
   b. Only Panita's private key (and no other keys)
   c. Panita's public key and Pongpak's public key
   d. Panita's private key and Pongpak's public key
   e. Panita's public key and Pongpak's private key
   f. Panita's private key and Pongpak's private key

Correct answer: (a)

An X.509 certificate only contains the users (e.g. Panita's) public key. Even though the certificate is signed with the CA's (Pongpak's) private key, the private key is not included. Also, although the CA's (Pongpak's) public key is needed by the user to verify the certificate, the CA's public key is not included in the user's certificate.

d) If user **A** has a X.509 certificate signed by CA **X** and user **B** has a X.509 certificate signed by CA **Y**:

   a. **A** and **B** can never authenticate each other
   b. **A** and **B** can only authenticate each other if **X** and **Y** exchange private keys
   c. **A** and **B** can authenticate each other if **X** and **Y** trust each other and exchange their public keys
   d. **A** and **B** can authenticate each other if the **A**'s certificate is sent to **B** (and vice versa)

Correct answer: (c)

If A and B use different CA's in X.509, they can authenticate by obtaining the certificates (public keys) of the other CA. For example, A needs to obtain the certificate of Y from X. For this to happen, X and Y must exchange public keys (certificates) – which implies they must trust each other (or have a higher authority to sign the certificates).

Question 3 [2 marks]

a) In IPsec what are two security services provided by *both* Authentication Header (AH) and Encapsulating Security Payload (ESP)?

Both AH and ESP provide: **authentication and integrity**. Other acceptable answers would be access control or anti-replay or key management (although the last two aren't considered as core security services).

b) What security service can be provided by ESP, but not by AH?

ESP can also provide **confidentiality** (or privacy).

Question 4 [2 marks]

a) What is the difference between a Hash function and a Message Authentication Code (MAC) function?

A MAC function takes as input the Data and Secret Key, while a Hash function only operates on the Data.

b) What can be used to convert most hash functions to MAC functions?

HMAC is a function that converts most Hash functions into MAC functions. That is, it allows you to use a Secret Key with your Hash function. (The reason for doing this is that many Hash functions are well supported, e.g. freely available code and well understood, and so it makes sense to use them as a MAC as well).