**TNE30024**

Deploying Secure Engineering Applications Online

**Tutorial 4 (week 5)**

**Applications of PKI**

**Questions**

1. When purchasing goods via a website, why does the SSL/TLS protocol require the website to provide a digital certificate but not the person doing the purchasing?

SSL/TLS requires the website to provide a digital certificate to establish a trust relationship with the client (the purchaser). The certificate ensures that the client is communicating with the legitimate server that owns the domain. This prevents impersonation and man-in-the-middle attacks. Clients, typically consumers, do not provide certificates because they are not hosting services and identity verification is handled at the application layer (e.g., through usernames and passwords).

1. Public key cryptography is rarely used for encrypting raw data. Why?

Public key cryptography involves more complex mathematical computations than symmetric key cryptography, making it significantly slower. Therefore, it is not generally used for encrypting large amounts of data due to performance issues. Instead, it's primarily used to encrypt small data like symmetric keys or to provide digital signatures and key exchange mechanisms.

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 (Challenge-Handshake Authentication Protocol) avoids transmitting passwords in the clear by using a challenge-response mechanism. When a session starts, the server sends a challenge to the client. The client uses a hash function to combine the challenge with its password and sends the result back to the server. The server performs the same hash calculation on its side to verify. This method means the password itself is never sent over the network.

1. CHAP requires both parties to authentication to have a shared secret whereas authentication based on PKI does not require any shared secret information. Explain why.

CHAP requires both parties to know the secret (password) because it uses this shared secret to generate the response to the challenge, verifying the identity without transmitting the secret itself. PKI (Public Key Infrastructure), on the other hand, relies on digital certificates and a pair of public and private keys. The public key, which is openly distributed via certificates, allows anyone to encrypt a message to the holder of the private key or verify a message signed by them. There is no need for a shared secret because the security is based on the private key remaining confidential with its owner.

1. Consider a simple challenge response authentication scheme as follows:

To calculate the response to the challenge, the challenge is encrypted using a stream cipher and the result returned is the response to the challenge.

Recall that stream ciphers generate a pseudo-random number sequence (PRNS) which is then XORed with the plain text to become the cipher text.

If the stream cipher generates a PRNS of 00010101 in binary what will be the response to a challenge of 7 (in decimal)?

Express your answer in decimal and use a diagram to show the exchange of messages.

If the stream cipher generates a PRNS of 00010101 and the challenge is 7 (in decimal, which is 00000111 in binary), the response is calculated as:

PRNS ⊕ Challenge = 00010101⊕ 00000111 = 00010010

Converting the binary response 00010010 back to decimal gives 18.

Client Server

| |

|----Send Challenge (7)-------> |

| |

|<---PRNS (00010101)---------- |

| |

|----Response (18)------------> |

| |

1

1. IPSec requires a substantial overhead in terms of additional headers and trailers.
   1. How many additional bytes are required if the packet is transmitted via IPSec using transport mode and encapsulated using AH?

 **IP Header:** 20 bytes

 **AH Header:** 32 bytes (256 bits)

 **Total Additional Bytes:** 52 bytes

* 1. How many additional bytes are required if the packet is transmitted via IPSec using tunnel mode and encapsulated using ESP?

 **New IP Header:** 20 bytes

 **ESP Header:** 4 bytes (32 bits)

 **ESP Trailer:** 4 bytes (32 bits)

 **ESP Authentication:** 20 bytes (160 bits)

 **Original IP Header (encapsulated):** 20 bytes

 **Total Additional Bytes:** 68 bytes

The following might be useful:

* + IP packet header (IPv4) is 20 bytes
  + AH header is 256 bits
  + ESP header is 32 bits
  + ESP trailer is 32 bits and
  + ESP authentication is 160 bits.

You will need to review the notes to refresh your memory of tunnel and transport mode formats.

2