SWINBURNE UNIVERSITY OF TECHNOLOGY

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?

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

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

4) 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.

5) 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.

6) IPSec requires a substantial overhead in terms of additional headers and trailers.

   i) How many additional bytes are required if the packet is transmitted via IPSec using transport mode and encapsulated using AH?

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

   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.