Parker
Eischen

Homework 13

Review 22.4: DKIM - Domainkeys Identified Mail is a type of cryptographically signing emails. This allows emails to be claimed in a mailstream. This is used to verify senders of mail similar to the public key system

Review 22.5: SSL can be comprised by the Handshake Protocol, Alert Protocol, the change cipher - Spec Protocol and (HTTPS)

Problem 22.5

Mode 1: Transport mode
- it a host may Authentication Header or Encapsulating Security Payload over Internet Protocol version v 4 (IPv4) then the payload is the data
- AH in transport mode in some portion of IP header and can authenticate IP header

Mode 2: Tunnel Mode
- packets can have different source and destination addresses
- firewall implements the IPSec then the tunnel mode is received in both ends of SA

Review 23.9: Public key infrastructure - Provides all components needed for entities to communicate securely

Problem 23.4

https://youtube.com

Problem 23.4: https://www.youtube.com

Public key:
04 9b 10 94 f4 1b 2a e3 1b 05 5f 71 b8 56 48 50 0a 67 60 cf 3e 33 08 a5 68 6e 84 e3 ec 69 7f 14 87 33 60 4e c5 b3 9e 30 7f b0 b7 ff 09 41 85 49 6a dc 3a 6b 68 96 a9 92 6f e6 3d ff 0a a2 78 15 aa

Issuer:
CN = Google Internet Authority G3
O = Google Trust Services
C = U

Issued: Wednesday, November 7, 2018 1:59:00 AM
Valid: Wednesday, January 30, 2019 1:59:00 AM
Signature type: sha256RSA
CA certificate
Certificate is currently valid
No obvious problems in this certificate

Problem 23.5: Arduino Certificate

Public key:
04 7a 3a e8 4d 29 21 55 d7 2d 24 0f aa 70 e2 fa bc 48 5a 80 25 5d 6a 38 34 55 12 25 4b ff 18 37 52 6f 7d be 4c 45 c2 4c 0b 16 c7 20 17 c0 0c 7d 9f 94 b8 33 66 6c 96 cc 38 b9 00 35 f6 55 df 6b 95

Issuer:
CN = Arduino
OU = IT
O = Arduino LLC US
C = US

Issued:Monday, August 14, 2017 11:04:03 PM
Valid:Wednesday, August 14, 2019 11:04:03 PM
Signature type: sha256ECDSA
CA certificate
Certificate is currently valid
No obvious problems in this certificate