Computer Networks
Jacobs University Bremen
Dr. Jürgen Schönwälder

Course: 320301
Date: 2013-12-06
Time: 10 min.

Quiz Sheet #6

Problem 6.1: *cryptography* (1+3 = 4 points)

a) Explain the difference between a symmetric cryptosystem and an asymmetric cryptosystem.

b) What distinguishes a cryptographic hash function from a regular hash function?

Solution:

a) A symmetric cryptosystem uses a key shared by both parties while an asymmetric cryptosystem uses a pair of keys, one key is public and used for encryption while the other key is private and used for decryption. Asymmetric cryptosystem simplify key management but tend to be computationally more expensive. Hence, asymmetric cryptosystem are often used to authenticate parties while creating session keys for use with symmetric cryptosystems.

b) For a cryptographic hash function H, it is should be difficult to

   (a) find a clear-text m such that $H(m)$ matches a given value h

   (b) find a clear-text m_2 for a given clear-text m_1 with $m2 \neq m_1$ such that $H(m_1) = H(m_2)$

   (c) find two different clear-texts m_1 and m_2 such that $H(m_1) = H(m_2)$

Problem 6.2: *IP layer security (IPsec)* (1+1 = 2 points)

a) Briefly explain the difference between transport-mode and tunnel-mode.

b) Which security services are provided by the AH header and which security services are provided by the ESP header.

Solution:

a) Transport-mode IPsec provides end-to-end security between two IP nodes by using an IPsec header inserted right after the IP header. Tunnel-mode provides a secure tunnel, which typically only covers a part of the end-to-end path. Tunnel-mode encapsulates an IP packet in another protected IP packet.

b) The AH header provides integrity protection and data origin authentication (and optionally replay-protection). The ESP header provides in addition payload encryption.

Problem 6.3: *transport layer security* (1+1 = 2 points)

a) What is the purpose of an X.509 certificate?

b) What is TLS session resumption?

Solution:

a) An X.509 certificate carries a public key including meta data such as the identification of the subject, the issuer, the time period in which the key is valid, and a serial number. An X.509 certificate also carries a signature proving the correctness of the certificate.

b) Establishing a TLS session involves computationally intensive operations in order to establish session specific keys. Normally, the session state is lost when the underlying TCP connection is closed. The TLS session resumption mechanism allows to maintain the TLS session state so that a subsequent TLS session can be established more efficiently by resuming a previously terminated TLS session.

Problem 6.4: *secure shell* (1+1 = 2 points)

a) What is the purpose of an SSH host key?

b) What are SSH channels? Provide an example what they might be used for.

Solution:

a) An SSH host key identifies the host an SSH server is running on. It is used to verify that the connection initiated by an SSH client has reached the correct host.

b) SSH can multiplex multiple independent channels over a single TCP connection. This can be used to support the forwarding of X11 traffic (GUI applications) over an SSH remote login. It can also be used to leverage an existing SSH connection for multiple remote logins or file transfers.