IK2206 – Internet Security and Privacy

Assignment 3

Exercise 1

Which of the following statements about web security are true?

☐ a. A hash of username + password is a good authenticator in cookies.

☑ b. User input should always sanitized before used.

☑ c. Cross-site scripting attacks rely on weak validation of user data. [1]

☐ d. Cookies are used to execute code in the client browser.

☑ e. Javascript uses same-origin policy to protect against cross-site scripting attacks.

Exercise 2

Which of the following statements about TLS are true?

☐ a. Protects against spoofed IP-addresses. [2]

☐ b. Provides only authentication of client and server

☑ c. Is dependent on a PKI to protect against spoofed identities. [3]

☐ d. Security can be defeated using chosen-protocol attacks. [4]

☑ e. Needs version checks in handshake to protect against version rollback.

Exercise 3

SSL/TLS starts with an initial handshake. The design of this handshake is very important for security, and it has been revised several times. Answer the following questions, concerning the latest versions of the protocol (SSL 3.0/TLS 1.2):

How are the keys for session encryption established?	By deriving information from the master secret ▼
How are the session encryption algorithms established?	By the cipher suite negotiation ▼
How are Cipher suite rollback attacks avoided? [5]	By using Finished messages ▼
How are version rollback attacks avoided?	By including control information in the generated secret ▼

[1] Weak input validation is required to inject the code into the target site's document to make this attack possible.

[2] Microsoft says it's not possible to spoof IP addresses when using TLS: http://technet.microsoft.com/en-us/library/gg195829.aspx. Our teachers say: "It does not protect against network-layer threats".

[3] http://en.wikipedia.org/wiki/Self-signed_certificate

[4] TLS protects the protocol selection to prevent chosen-protocol attacks. http://www.windowsecurity.com/uplarticle/2/chosen_protocol.pdf

[5] http://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS8a/SSLTLS.html

Exercise 4

Alice wants to send a confidential, authenticated email to Bob using PGP. This involves several steps of encryption and hashing operations. In which order are they done? [6]

First step: Hashing ▾

Second step: Encryption w ith Alice's private key ▾

Third step: Encryption w ith session key ▾

Fourth step: Encyption w ith Bob's public key ▾

Exercise 5

Internet's email protocols have remained the same for many years. With Internet's current email protocols, which of the following are possible?

☑ A. Setting up any host on the Internet as a mail relay

☑ B. Send email with fake "From" address

☑ C. Relaying an email via an external SMTP server, thereby hiding the sender's IP address

☑ D. Mix encrypted data and clear text data in the same email message

☑ E. Trick a computer to send spam without its owner noticing

Exercise 6

Assume that Alice would like to send Bob a confidential email using PGP. What is true for the *session key*, that is, the key that Alice uses to encrypt the message?

● a. The session key is generated by Alice, and encrypted with Bob's public key

○ b. The session key is generated by Alice, and encrypted with Alice's private key

○ c. The session key must be known by Alice and Bob before Alice sends the email

○ d. The session key is generated using a Diffie-Hellman key exchange

Exercise 7

With PGP's key infrastructure, certificate signatures are provided by:

○ A. A single, trusted CA

○ B. Any trusted CA, or any organization to which a trusted CA has delegated the right to sign

● C. Anyone

○ D. Any trusted CA

[6] See IK2206, lecture about email security, slide 23. The order in which the encryption process happens can potentially be parallized: The process of encrypting the session key can be performed in parallel to the message hashing and encryption process. Finally, both parts, the encrypted session key and the encrypted message (including message digest), can be sent out to the destined recipient.

Exercise 8

Which of the following statements about securing networks and hosts are true?

□ a. A VPN tunnel is required to access machines in the DMZ.

☑ b. It is advisable to set up externally visible services in a DMZ.

□ c. Bastion hosts must be dual-homed to protect the private network.

☑ d. Hosts on the private network should not trust or be accessible from machines in the DMZ.

☑ e. A bastion host should run only the services it is providing.

□ f. Bastion hosts must be deployed only in a DMZ. [7]

☑ g. Implementing an application-level gateway for a protocol is more difficult than using a packet filter.

Exercise 9

Which of the following statements about firewalls are true?

☑ a. Stateful packet filters allow more precise control over filtering.

□ b. Stateless packet filters can't filter based on the application protocol.

□ c. Application gateways can be used to protect against IP address spoofing attacks.

☑ d. An HTTP cache can be seen as an example of an application gateway.

□ e. Stateful packet filters can protect against SQL injection attacks.

Exercise 10

Which of the following statements about firewalls are correct?

☑ A. An application-level gateway can normally provide user-to-gateway authentication.

□ B. The default forward policy in packet filter firewalls is more conservative than the default discard policy.

□ C. Compared to application level gateways, packet filter firewalls provide strong user authentication mechanisms.

☑ D. Packet filters can make decisions based on multiple protocol level headers.

□ E. An application-level gateway is normally invisible to users and end systems. [8]

□ F. A single-homed bastion host configuration protects the internal network even if the packet filter is compromised.

[7] A bastion host is – by definition – accessible from the internet. Hence, it has to be separated from the private network. Such are usually done by using a DMZ. http://en.wikipedia.org/wiki/Bastion_Host.

[8] It hardly depends on what kind of firewall we're talking about.