IK2206 – Internet Security and Privacy
Assignment 2

Exercise 1
Nonces are frequently used in authentication protocols. What is true?

- [ ] A. Nonces need to be random numbers
- [x] B. Nonces are used for protection against replay attacks
- [x] C. A nonce should be used only once
- [ ] D. Nonces are shared secrets; therefore they should always be encrypted.
- [ ] E. Sequence numbers are predictable and therefore cannot be used for nonces [1]

Exercise 2
Alice wants to authenticate herself to get access to a server S. The authentication is done through Kerberos, so it includes KDC, a Key Distribution Center, and TGS, a Ticket Granting Server. The authentication process involves a number of different keys.

Complete the following statements:

The shared key between Alice and KDC	is computed from Alice's password
The shared key between Alice and TGS	is created by KDC
The shared key between TGS and S	is used to encrypt the Service Ticket
The shared key between KDC and TGS	is used to encrypt the Ticket Granting Ticket
The shared key between Alice and S	is created by TGS

Exercise 3
Kerberos is an authentication protocol widely used for different applications. What is true?

- [x] A. User passwords are never transmitted between client and server
- [x] B. A service ticket consists of information encrypted with the long term key shared by the ticket granting server and the server
- [ ] C. Kerberos uses public key cryptography for establishing a session key
- [x] D. The authenticator for a service request is encrypted with the short-term key generated by the ticket granting server
- [ ] E. The ticket granting ticket consists of information encrypted with a key generated from the user's password
- [x] F. Client-to-server authentication takes place by the client sending a ticket and an authenticator to the server
- [ ] G. A Kerberos Authentication Server stores user passwords in clear text
- [ ] H. The authenticator for the ticket granting server consists of information encrypted with the long term key between authentication server and ticket granting server

[1] Yes, they can. It is the "used once" property that is important.

Exercise 4

Alice wants to set up private communication with Bob. She therefore sends a request to a Key Distribution Center, KDC. The KDC returns to Alice, among other things, a *ticket*, which she sends to Bob together with an invitation to communicate. The ticket consists of encrypted data. Which key is used to encrypt the data?

- ○ A. Bob's public key
- ○ B. Alice's public key
- ○ C. The key shared by Alice and the KDC
- ○ D. The KDC's public key
- ◉ E. The key shared by Bob and the KDC
- ○ F. The key shared by Alice and Bob

Exercise 5

Which of the following statements about IKE are correct?

- ☑ A. IKE is used to do mutual authentication between sender and receiver.
- ☐ B. IKE defines what ciphers to use for secure communication.
- ☐ C. IKE assumes that both parties have a pre-established shared secret key. [2]
- ☐ D. IKE is vulnerable to replay attacks.
- ☑ E. IKE phase 1 consists of three parts: parameter negotiation, Diffie-Hellman exchange, and authentication.

Exercise 6

Which of the following statements about security associations (SA) are correct?

- ☐ A. The SA is a two-way relationship between sender and receiver.
- ☐ B. The SA must be established automatically through e.g., IKE.
- ☑ C. The SA can be manually configured.
- ☑ D. The SA specifies what cryptographic algorithm to use.
- ☐ E. The SA is included in the IPsec header.

[2] IKE uses a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.

Exercise 7

Which of the following statements about IPsec AH (Authentication Header) and ESP (Encapsulating Security Payload) are correct?

- [x] A. AH can authenticate parts of the IP header. [3]
- [x] B. ESP can encrypt the complete IP packet (header and payload).
- [x] C. ESP can be used both for confidentiality purposes and for authentication.
- [ ] D. With ESP in tunnel mode, a firewall inside the tunnel can always interpret the original IP header fields.
- [ ] E. AH can be used to authenticate the IP packet payload and the complete IP header.
- [ ] F. ESP works in tunnel mode only.

http://www.ciscopress.com/articles/article.asp?p=25474&seqNum=7
http://www.internet-computer-security.com/VPN-Guide/Tunnel-mode.html

Exercise 8

When used in authentication schemes, fingerprints...

- [ ] a. ...are subject to dictionary attacks.
- [x] b. ...are easy to forge.
- [ ] c. ...are resistant to false positives. [4]
- [x] d. ...cannot be revoked once enrolled. [5]
- [ ] e. ...is the best biometric method currently known.

Exercise 9

What kinds of threats does password hashing protect against?

- [x] a. Offline dictionary attack
- [ ] b. Shoulder surfing
- [ ] c. Eavesdropping
- [ ] d. Online dictionary attack
- [x] e. Password theft

Exercise 10

Password salting is a method to...

- ( ) a. ...make online dictionary attacks harder.
- (•) b. ...increase the cost of offline password guessing.
- ( ) c. ...replacing password hashes.
- ( ) d. ...defeat shoulder surfing attacks.
- ( ) e. ...increase the quality of passwords.

[3] In IPv4, the AH protects the IP payload and all header fields of an IP datagram except for mutable fields (i.e. those that might be altered in transit). Mutable (and therefore unauthenticated) IP header fields are DSCP/TOS, ECN, Flags, Fragment Offset, TTL and Header Checksum. (http://en.wikipedia.org/wiki/IPsec)

[4] The chance of a "false positive" (two different individuals having the same fingerprints) is about 1 in 64 billion. If this is not enough, a combination of multiple fingers can be taken to make the key more robust. (http://en.wikipedia.org/wiki/Fingerprint). For some reasons, the teachers still say, that fingerprints are not resistant to “false positives”.

[5] Fingerprints can actually be revoked once enrolled – but only in combination with a second authentication method (e.g. PIN code).