TTM4135 Information Security Summer Exam Aug. 12, 2004

Outline answers to questions and problems. (Version 2)

1. Short definitions
    a. *Covert channel* enables the transfer of information in a way unintended by the designers of the channel.
    b. *Discretionary access control* is means for restricting access to objects that can be decided and set by the *owner* of the objects "at her own discretion".
    c. ISAKMP is short for Internet Security Association and Key Management Protocol, a framework for key exchange in IPsec. *Oakley* is a key exchange protocol based on Diffie-Hellman mandated for use within ISAKMP.
    d. *Multilevel security* is a mandatory security policy that enforces access control based on classification levels of subjects and objects.
    e. *Unconditionally secure* means secure even against an opponent with unlimited computing time and resources. Synonymous with information-theoretic secure.
    f. ITU-T recommendation X.509 defines a framework for the provision of authentication services of the X.500 directory. In particular, it defines a public-key certificate structure and authentication protocols.
2. Textbook Figure 11.1 page 347 illustrates the three common types of firewalls: packet filters, application-level gateways, and circuit-level gateways.
3. Application data -> Fragmentation -> Compression-> Add MAC -> Encrypt-> Append SSL record header (Text book Figure 7.3)
4. To make it easy to change cipher without carrying out the whole Handshake protocol over again.
5. Principal services of Ipsec are access control, connectionless integrity, data origin authentication, rejection of replayed packets, confidentiality, and limited traffic flow confidentiality.
6. Transport mode is end-to-end security association, whereas tunnel mode is end-to-intermediate security association.
7. Protocol stack diagrams can be found in Textbook Figure 7.1 page 216.
8. See textbook Table 5.1. PGP principal services are performed in the following sequence at the senders side: Digital signature, Compression, Message encryption, E-mail compatibility (Radix-64 conversion), and Segmentation.
9. Algebraic definitions can be found in Textbook problem 5.1 page 159.
10. No, P_3=$\mathrm{D}_K(\mathrm{C}_3) + C_2$ and beyond are received correctly, under the assumption that C_2 and beyond are correct.
11. Source error in CBC mode
    a. All blocks from C_1 will contain an avalanche of bit errors compared to the correct ciphertext blocks. The ciphertext errors are unpredictable without knowing K because $\mathrm{E}_K(P_\mathrm{i} + C_{\mathrm{i-1}}) \rightarrow C_\mathrm{i}$
    b. One bit error equal to source.
12. PGP message digest.

    a. Not at all. The message digest is “encrypted” by a private key; hence it can be decrypted by the corresponding public key. SHA-1 is public and keyless in order for the verifier to be able to recompute the message digest from the received message.
    b. The probability of exact match of 16 bits using a wrong verification key is 2^{-16}. Of course, the message signature verifies only if the remaining 146 bits also match the recomputed message digest. In addition, the 64 least significant bits of the sender’s public key are included in the signature header too.

13. An eavesdropper can compute the secret key from the two messages sent.
14. Several solutions are possible and acceptable, but it is not necessary to introduce new secret keys in the protocol. A simple solution would be for Bob to send $h(K_B)$ and for Alice to check whether $h(K_A)$ matches.
15. 253 = 11 x 23. d = 1/13 mod phi(11*23) = 1/13 mod 220 = 17.
16. 2^17mod 253 = 18.
17. Personal data: All data that can be linked to a physical person.
    Personopplysning: Alle opplysninger som <u>kan</u> knyttes til en fysisk person.
18. “Behandling av personopplysninger” = “alle” operasjoner som kan utføres på en personopplysning. Loven gjelder når behandlingen skjer “<u>elektronisk</u>” eller er knyttet til et “<u>register</u>”.
    a. Må alltid ha rettslig grunnlag for å behandle personopplysninger:
        i. Lovhjemmel
        ii. Samtykke (informert, eksplisitt, frivillig)
        iii. Nødvendig grunn (slik § 8 i loven angir)
    b. Må alltid på forhånd ha fastlagt et <u>formål</u> for behandlingen
    c. Må alltid på forhånd ha gjennomført vurderinger av informasjonssikkerhet, internkontroll og opplysningskvalitet.