Mid-term Exam (ANSWERS)
Information Security, 08 March 2018

Question 1 (22 points)

(a) There are two types of assets that information and computer security aims to protect: software and hardware

A. True
B. False

Answer: B

(b) The three basic elements of access control are

A. subject, objects and permissions
B. objects, access modes and rights
C. subjects, objects and access modes
D. subjects, access modes and permissions

Answer: C

(c) Skimming is the use of a/an ______ to ______ authentication data without being noticed

A. device
B. password
C. mobile phone
D. move
E. delete
F. copy

Answer: A, F

(d) Determine which of the following characteristic(s) apply to AES

A. The block size is 128 bits
B. It operates only with 16 rounds
C. It employs bit shifting as an encryption primitive
D. The key length can reach 112 bits with multiple keys

Answer: A

(e) Determine if the following sentences about network protocols are true or false:

A. They provide the details on how communication is accomplished
B. They enable the independence between communications and the communication medium
C. They are conventions for computers to interact

Answer:
A. False B. True C. True

(f) Which statement is true or false?
An intrusion detection system:

A. looks for intrusions before the packets are inspected by the firewall

B. if host-based, it is installed on a dedicated machine that protects the entire network

C. operates before an attack has begun

Answer:
A. False B. False C. False

(g) An attacker exploits a/an ___ in order to cause a/an ___. A/an ____ blocks a vulnerability by removing or reducing the effect of a/an____

A. attacker
B. vulnerability
C. threat
D. countermeasure
E. defender
F. obstacle
G. bug

Answer: B, C, D, C

(h) How many attack attempts are necessary in the worst case to decrypt a message written in English encrypted with the Caesar cipher? ___

Answer: 25

(i) Determine whether the following statements refer to block ciphers or stream ciphers

A. The input symbols are transformed one at a time

B. The speed of transformation is high because symbols are encrypted as soon as they are read

C. Padding is typically required for most messages

Answer: A. stream B. stream C. block

(g) In an echo-chargen attack, the attacker sets up a/an ___ on one machine that generates a/an ____ that targets another machine. This creates a/an ____ between two machines.

A. large packet
B. chargen process
C. echo packet
D. echo process
E. communication loop
F. smurf process
E. vulnerability
G. authentication problem

Answer: B, C, E

2. (6 points) If you forget your password for a website and click `Forgot my password`, sometimes the company/service provider sends you a new password by email but sometimes it sends you your old password by email. Compare these two cases in terms of vulnerability of the website owner.

Answer: If the site tells you what your password was, that means the site is storing your password rather than just a hash of it. This means that anyone who gains access to the site's password database has access to all the passwords. If the site sends you a temporary password, there is a good chance it is not storing actual passwords, which is the correct approach from a security perspective.

3. (5 points) IPsec can enforce confidentiality and/or authenticity via two modes of operation. State and briefly describe each of them, including how the recipient's address is protected.

Answer:
Transport mode: IP address header is unencrypted
Tunnel mode: recipient's address is concealed by encryption and IPsec substitutes the address of a remote device that will receive the transmission and remove the IPsec encryption

4. (3 points) Does a VPN use link encryption or end-to-end encryption? Justify your answer.

Answer: VPN uses both link and end-to-end encryption.

The methodology for the communication security which is used for encryption and decryption of all the traffic at both ends of the communication is known as link encryption.

The methodology that is used for the confidentiality and integrity of the data is transmitted by encryption at start point of the communication line and decryption at the end point of the communication line is known as end-to-end encryption.

5. (6 points) Consider circuit switching and packet switching. What are the benefits of each of them? Mention at least two for each.

Answer:
Circuit switching: Dedicated end-to-end connection, fixed, reliable transmission rate.
Packet switching: Better sharing of transmission capacity, more users, less idle period, better handling of data burst, on demand, easier and cheaper implementation

6. (4 points) A circuit in a link is implemented with either frequency division multiplexing (FDM) or time-division multiplexing (TDM). What is the main difference between FDM and TDM? What are particular circuits assigned to?

Answer: FDM divides the link along the frequency spectrum, each circuit being provided with a fraction of the bandwidth, while TDM divides the link along time frames, further divided into slots allocated to different circuits.

7. (9 points) You receive an email message that claims to come from your bank. It asks you to click a link for some reasonable-sounding administrative purpose.
(a) How can you verify that the message did come from your bank?
(b) Now play the role of an attacker. How could you intercept the message described in part (a) and convert it to your purposes while still making both the bank and the customer think the message is authentic and trustworthy?

Answer: Some ***main ideas*** *(must be elaborated further) for possible answers are:*
(a) Confirm that both the "from" address and the link provided in the email precisely match the domain belonging to the bank.
Check for obvious signs of email phishing; check email header
(b) By changing something minor with the domain (e.g., .co instead of .com) or intercepting the DNS request from the customer (via a man-in-the-middle-attack). The link will then redirect to the legitimate page while allowing the attacker to perform whatever malicious behavior is desired.

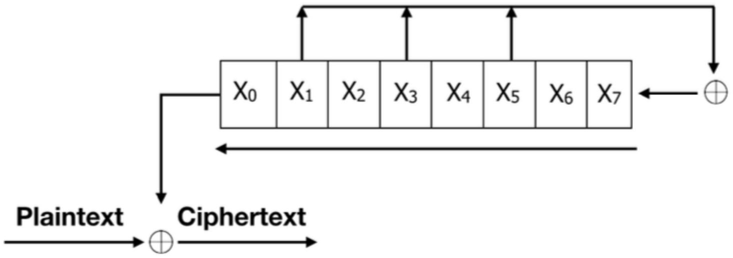
8. (14 points) State and briefly describe the different layers of the OSI reference model, and give an example of a protocol used at each layer

Answer:

Physical layer	Defines the electrical and physical specifications of the data connection	Coax/fiber/wireless
Data link layer	Provides node-to-node data transfer	Ehternet/SLIP/PPP/FDDI
Network layer	Routing of datagrams from source to destination	IP/IPSec/ICMP/IGMP
Transport layer	Provides functional and procedural means of transferring variable-length data sequences from a source to a destination host	TCP/UDP/ECN/SCTP/DCCP
Session layer	Provides long-lasting communication sessions between applications	APIs/SOCKETS

Presentation layer	Formats and delivers information to the application layer for further processing	SSL/FTP/IMAP/SSH
Application layer	Specifies shared protocols and interface methods used by hosts to communicate	HTTP/FTP/IRC/SSH/DNS

9. (12 points) Consider the following simple Linear Feedback Shift Register (LFSR). The plaintext is bitwise XOR-ed with the output bits of the LFSR which first computes X1 ⊕ X3 ⊕ X5 and then shifts such that X0 falls out. Compute the next three states of the LFSR given the initial state 00111010. You need to clearly show (i) each state, (ii) the output bit, and (iii) your XOR computation



Answer:

Initial state = 0011 1010

0 xor 1 xor 0 = 1

Output = 0

Next state: 0111 0101

1 xor 1 xor 1 = 1

Output = 0

Next state: 1110 1011

1 xor 0 xor 0 = 1

Output = 1

Next state: 1101 0111

10. (19 points) Alice has chosen primes, p = 17 and q = 23, and encryption exponent, e = 5 as her RSA parameters

(a) Alice digitally signs message m = 10 and sends it to Bob. Show all the intermediate steps of your solution and explicitly mention what Alice sends to Bob.

(b) Bob receives the signed message and proceed to verify it. Show how Bob can verify the signed message. Write down all the intermediate steps of your solution.

$p=17 \quad q=23 \quad n=391 \quad e=5$

$\phi(n) = (p-1)(q-1)$

$= 16 \cdot 22 = 352$

(a) $m=10$

Alice computes: $y = m^d \bmod n$

$d = e^{-1} \bmod \phi(n)$

$= 5^{-1} \bmod 352$

using EA:

$352 = 70\times5+2$ — ②

$5 = 2\times2+1$ — ①

$2 = 2\times1+0$

using EEA:

From ①: $1 = 5-2\cdot2$ — ③

from ②: $2 = 352 - 70\cdot5$ — ④

Substitute ④ in ③

$1 = 5 - 2(352-70\cdot5)$

$= 5 - 2\cdot352 + 140\cdot5$

$= 141\cdot5 - 2\cdot352$

working mod 352:

$1 = 141\cdot5 \bmod 352$

$\therefore 5^{-1} = 141 \bmod 352$

$\therefore d = 141$

Back to $y = m^d \bmod n$

$= 10^{141} \bmod 391$

Apply modular exponentiation:

$10^1 \bmod 391 \equiv 10$

$(10^1)^2 = 10^2 \bmod 391 \equiv 100$

$(10^2)^2 = 10^4 \bmod 391 \equiv (100)^2 = 225$

$(10^4)^2 = 10^8 \bmod 391 \equiv (225)^2 = 186$

$(10^8)^2 = 10^{16} \bmod 391 \equiv (186)^2 = 188$

$(10^{16})^2 = 10^{32} \bmod 391 = (188)^2 = 154$

$(10^{32})^2 = 10^{64} \bmod 391 = (154)^2 = 256$

$\therefore 10^{141} = 10^{64}\cdot10^{64}\cdot10^{8}\cdot10^{4}\cdot10^{1}$

working mod 391:

$= 256\cdot256\cdot186\cdot225\cdot10$

\/ mod 391

$= 239\cdot186\cdot225\cdot10$

\/

$= 271\cdot225\cdot10$

\/

$= 370\cdot10 \bmod 391$

$= 181$

Hence, $10^{141} \bmod 391 \equiv 181$

Alice send $(m,y) = (10, 181)$

(b) Bob knows $(m, y) = (10, 181)$ and proceeds to Verify the message:

$$Z \equiv y^{e_A} \bmod n_A$$
$$= 181^5 \bmod 391$$

$181 \bmod 391 = 181$

$181^2 \bmod 391 = 308 \equiv -83$

$(181^2)^2 = 181^4 \bmod 391 = (-83)^2 \equiv 242$

$\therefore\ 181^5 = 181^1 \cdot 181^4$

working mod 391:

$= 181 \cdot 242 \bmod 391$

$\equiv 10$

$\therefore\ Z = 10 =$ message, m.