IS2150/TEL2810 Introduction to Computer Security
Final Examination
Tuesday, December 13, 2005

Name:

Email:

Total Time : 2:30 Hours
Total Score : 100

The questions have been grouped into two parts. The first part is worth 25 points and the second part is worth 75 points. The second part has each questions worth 3 points.

Be concise in your answers.

Score: ______________________

***Good Luck*!!**

Part I [Total points 25 = 15 + 10]

1. Indicate T for *True* or F for *False*; *Circle* the right answer from the given choices; Or fill in the blank.

    1. [ ] The product of two relatively prime numbers is a prime.

    2. [ ] For an RBAC configuration with no role hierarchy, *assigned_users*(*r*) and *authorized_users*(*r*) would be the same each role *r*.

    3. [ ] Even if each security domain is secure, when we allow cross-domain accesses, they can introduce security holes in a system.

    4. [ ] In *known plaintext* attack, the attacker's primary goal is to find the key *K* used.

    5. [ ] Cæsar is a transposition cipher and its key weakness is that the key is too short.

    6. [ ] The key to attacking Vigenere cipher is to find out the *period* of the key.

    7. [ ] If (RS, n) = ({$r1$, $r2$, $r3$}, 2) defines a DSD constraint, then the user assignment UA = {(u, $r1$), (u, $r2$)} is not valid.

    8. [ ] $D_k(E_k(D_k(y))) = E_k(D_k(E_k(z)))$ for $y = E_k(x)$ and $z = (D_k(E_k(x)))$, where E_k and D_k refer to the encryption and decryption operation using key k.

    9. [ ] One weakness of *TCSEC* is that it is based heavily on *integrity* requirements and ignores *availability*.

    10. [ ] *Common Criteria* has a component that addresses country specific security evaluation needs of some nations.

    11. If $p = 44$, then $\phi(p)$ = ___________

    12. For key $k = 23$, the Caesar ciphertext for the message "ATTACKED" is

        _________________ .

    13. The mechanism to hide relatively small amounts of data in other significantly larger files is known as _____________________.

    14. The *setuid* bit in the UNIX file system has the following effect on a file:
        a. Allows any user to read, write and execute access the file.
        b. Denies all users except the owner to access the file.
        c. Causes the execution of the file to have the UID of the owner.
        d. Causes the file to run with UID of the user who executes.
        e. none of the above

15. Which of the following give *execution* right over “hello.txt” to *owners* and *group* members only?
    a. `chmod 4755 hello.txt`
    b. `chmod u+srwx g+rw o+r hello.txt`
    c. `chmod u=rwx, g=rwx, o=rx hello.txt`
    d. All of the above
    e. None of a, b and c

2. *Define* and *differentiate* (do any ***five*** of the following):

1. *Unconditionally Secure* **vs** *Computationally Secure*

2. *Open design* **vs** *Economy of mechanism*

3. *Virtual Private Network* **vs** *Demilitarized zone* (DMZ)

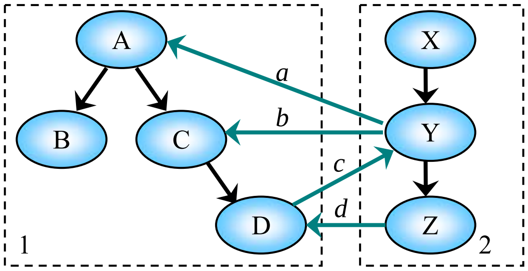
4. *Macro virus* **vs** *TSR Virus*

5. *Requirements Tracing* **vs** *Informal Correspondence*

6. *Structural Testing* **vs** *Functional Testing*

Part II (Total Score: 75 = 3 x 25)

1. Is this configuration for interoperation secure? Why? If not, what principle of secure interoperation is violated and how it can be made secure?



Answer:

2. Explain and give examples of how UID and EUID are effective in managing access control in UNIX systems.

Answer:

3. *Alice* wants to communicate with *Bob*. Let (E_A, D_A) and (E_B, D_B) be public-private key pairs of *Alice* and *Bob*. *Alice* wants to send a message to *Bob*. In the table, indicate the encryption/decryption expression to indicate what Alice or Bob would do for each requirement when *Alice sends M to Bob*. Use $E(M)$ and $D(M)$ to represent encryption using public and private keys of a message M. Let c be the cipher-text that *Bob* receives.

[a]	To ensure confidentiality of the message	*Alice* does (encryption): c = *Bob* does (decryption): M =
[b]	To ensure integrity of the origin of the message	*Alice* does (encryption): c = *Bob* does (decryption): M =
[c]	To ensure both integrity of origin and confidentiality of the message	*Alice* does (encryption): c = *Bob* does (decryption): M =

4. Consider the message blocks m_1, m_2, m_3. If the Cipher Block Chaining mode DES encryption can be expressed as follows:

$$c_1 = DES(m_1 \oplus \ ivector),\ c_2 = DES(m_2 \oplus \ c),\ c_3 = DES(m_3 \oplus \ c_2)$$

where *ivector* is the initial vector and ⊕ is the XOR operation

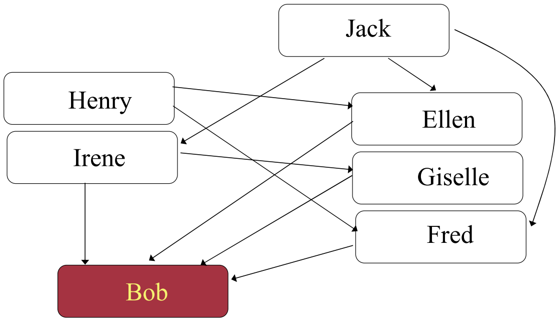
Write the expressions for the DES decryption to extract each of the message blocks m_1, m_2, and m_3.

Answer:

$m_1 =$
$m_2 =$
$m_3 =$

5. Write the *simple key exchange* protocol involving *Alice*, *Bob* and the trusted party *Cathy*, where *Bob* initiates the communication with *Cathy* to get the session key.

6. Recall the OpenPGP certification system. Briefly describe, using the following diagram as an example, how the certificate validation works. Can Bob's certificate ever be validated by the signature chain *Bob<<Giselle>>Giselle<<Irene>>Irene<<Jack>>*? Give reasons.

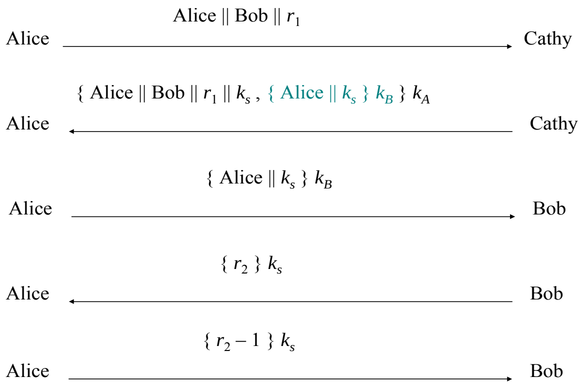


Arrows show signatures; Self signatures not shown

Answer: (Provide on the adjacent blank side)

7. Recall the Needham-Schroeder protocol as shown below. Suppose *Eve* can obtain the session key, what type of attack can she launch? Illustrate the attack with a diagram.

Answer:



8. What is a *dictionary* attack? Briefly describe the two types of *dictionary* attacks.

Answer:

9. For the *S/Key* scheme for password authentication, write the following:

   a. If *h* is the hash function used,

      (i) the *n* keys, k_1, k_2, .., k_n are generated as follows:

      ____

      (*ii*) the keys are used in the following sequence:

      ____

   b. Explain why the attacker cannot determine the next password the user will use by capturing the current communication:

   Answer:

10. What are the three required properties of a *reference validation mechanism*?

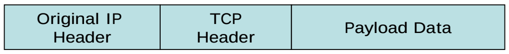
Answer:

11. Briefly explain and differentiate among the following: *functional*, *structural*, *unit* and *system* testing

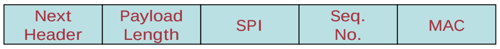
Answer:

12. Show how the IPSec packets look for each scheme (AH and ESP in Transport and Tunnel modes and briefly explain what is achieved by each scheme two IPSec protocols in two different modes. The following diagram show different pieces to start with.

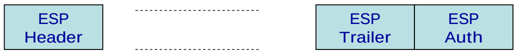
Answer (Use this and the adjacent blank page)



Without IPSec



Authentication Header (AH) Parameter



Encapsulating Security Payload (ESP) components

13. Recall that we use constraint p_i: *action* $\Rightarrow$ *condition* to determine what needs to be audited. *Justify* that the following constraint for the *Chinese Wall Policy* works and state what needs to be recorded.

Constraints

- $S \textit{ reads } O \Rightarrow COI(O) \neq COI(S) \vee CD(O) \in CDH(S))$
- $S \textit{ writes } O \Rightarrow (S \textit{ canread } O) \wedge \exists\neg O'(CD(O) \neq CD(O') \wedge S \textit{ canread } O' \wedge \neg sanitized(O'))$ (*Note: sanitized(O) iff O contains only sanitized information*)

Answer:

14. Let *U* be a set of user, *P* be a policy that defines a set of information *C*(*U*) that *U* cannot see. What do you mean by the following? Also show how a sanitizer can be used to address these:

- *P* is such that "*C*(*U*) can't leave site"

Answer:

- *P* is such that "*C*(*U*) can't leave system"

Answer:

15. Give reasons *for* and *against* doing risk management/analysis.
Answer:

16. For the risks and the security mechanism indicated below, calculate and insert the values as per the given data:
    - Risks:
        - disclosure of company confidential information,
        - computation based on incorrect data
    - Cost to correct data: $8,000,000
        - @25% liklihood per year: __2,000,000______
        - Effectiveness of access control software: 60%: -$1,200,000
        - Cost of access control software: +$55,000
        - Expected annual costs due to loss and controls: ________
        - Savings: ________

17. Write differences among *copyright*, *patent* and *trade secret*.

Answer:

18. Recall the following example of a *Trojan horse*

- *Perpetrator*

```
cat >/homes/victim1/ls <<eof
cp /bin/sh /tmp/.xxsh
chmod u+s,o+x /tmp/.xxsh
rm ./ls
ls $*
eof
```

That is, the perpetrator creates a file called ls in *Victim1*'s home directory
That is, when *Victim1* executes the file ls, he will be running a Trojan horse created by the *Perpetrator*.

(a) Explain what happens when *Victim1* executes the ls command while he is working in his home directory:

Answer:

(b) Suppose *Perpetrator* wants to make sure that once *Victim1* executes the Trojan horse ls, it propagates to *Victim2*. How may he change the above script to achieve it? You can write *pseudo code* and indicate where the additional code needs to be inserted in the script above.

Answer:

19. What are the steps involved in the *Flaw Hypothesis* methodology?

Answer:

20. Define the mathematic properties of the cryptographic checksum/hash function *h*: *A*→*B*:

Answer: (Provide on the adjacent blank side)

21. Recall the problem that we discussed in the class regarding the problem with *xterm* program. As a solution to the problem, the following check is done when *xterm* writes to the log_file – i.e., the process checks if the user running the *xterm* program can access the log_file; if yes, then the log_file is opened for writing. [1, 2]

```
if (access("log_file", W_OK) == 0)
        fd = open("log_file", O_WRONLY|O_APPEND)
```

Briefly describe why the above check still makes *xterm* vulnerable to "race condition".

Answer:

22. Briefly describe what you mean by the *emergent faults*.
Answer:

23. Briefly describe the different types of *intrusion detection* systems and intrusion handling techniques
Answer:

Answer *two* of the questions 24, 25, and 26

24. What is the TEMPEST program? Name two ways of protecting against emanations.
Answer:

25. Identify two natural disasters and state how one may protect information system resources against them.
Answer:

26. Enumerate two key elements that a security plan should address and state what they mean.
Answer: