IS2935 Introduction to Computer Security
Final,
Thursday, December 11, 2003

Name:

Email:

Total Time : 2:30 Hours
Total Score : 100

The questions have been grouped into four parts. These parts roughly correspond to the different sets of chapters as I had indicated in the class.

Part 1: (Total Score 20)
Part 2: (Total Score 25)
Part 3: (Total Score 30)
Part 4: (Total Score 25)

Note that scores for each question may be different – *so spend time accordingly on each question*. Be precise and clear in your answers.

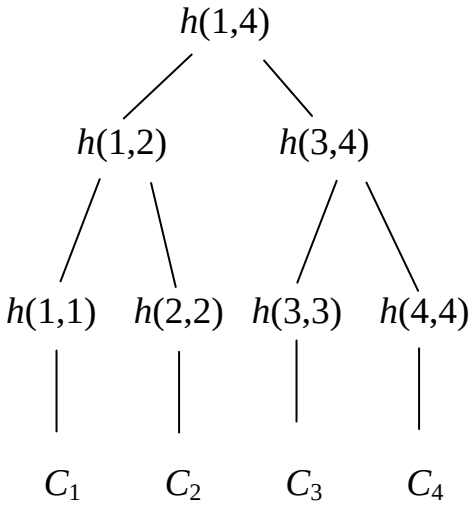
Score

Part 1	Part 2	Part 3	Part 4
Total:			

Best of Lucks!!

Part I: Certificates, Authentication and Identity (Total Score 20)

1. Refer to the Merklee's tree shown below. [1, 3]
   a. Indicate the hash values that need to be computed (use *circles*) and that need to be obtained (use *rectangular* boxes) to validate C_3



   b. At the time C_3 is being evaluated, suppose that C_1 gets corrupted. How does it affect the validation of C_3? Assume that the hash values are all available in the same file, but the certificates are not. Provide enough arguments to substantiate your point.

2. Recall that *X*<<*Y*>> represents *Y*'s certificate signed by *X*. Consider the following certificates and answer the following [2, 2]
   - *Dan*<<*Alice*>>
   - *Cathy*<<*Bob*>
   - *Dan*<<*Cathy*>>
   - *Cathy*<<*Dan*>>

   (a) Show steps (or just write the *signature chain*) that Alice takes to validate Bob's certificate:

(b) Show steps (or just write the *signature chain*) that Alice takes to validate Bob's certificate:

3. What is a *dictionary* attack? Briefly describe the two types of dictionary attack. [4]

4. Provide argument(s) *for* or *against* the following statement: [2]
   "*Use of salt increases the effort needed to launch dictionary attack.*"

5. For the *S/Key* scheme for password authentication, write the following: [2, 2].

a. If h is the hash function used,
   (i) n keys $k_1, k_2, .., k_n$ are generated as follows:

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

   ---

b. Assuming that h cannot be inverted, the attacker cannot determine the next password because of the following reason:

6. Identify two biometric authentication systems and give examples of attacks on them. [2]

Part II: Design Principles, Assurance (Total Score 25)

1. Write what the following design principles mean. [10]

   Fail-safe defaults

   Open design

   Economy of mechanism

   Psychological acceptability

   Complete mediation

2. What do you mean by *operational assurance*? State its importance. [2]

3. What are the three required properties of a *reference validation mechanism*? [3]

4. Five two characteristic of each of the following models of software development: [4]

    a. Extreme programming

    b. System assembly from reusable components

5. Briefly write about two ways checking that *design meets requirements* specified for a system. [2]

6. Indicate true or false for the following. [4]
    a. The following are desirable implementation considerations for *operational* assurance:
        i. Modularity [ ] True [ ] False

        ii. Low level language for implementation [ ] True [ ] False

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

    c. Common Criteria has a component that addresses country specific needs of some nations. [ ] True [ ] False

Part III: Network Security, Auditing, Risk Management, Legal/Ethical Issues (Total Score 30)

1. What are the functions of the following components of the *Secure Socket Layer* protocol? [1, 1]

    d. SSL Record Protocol

    e. SSL Handshake protocol

2. Provide argument(s) *for* or *against* the following statement: [2]
   "*IPSec is strictly independent and strictly an end-to-end protocol between two application level entities*"

3. Differentiate between the following [2, 2]

    a. The two IPSec protocols.

    b. The two IPSec modes

4. State what you understand by the following: [2]

    a. *Security Association Bundle*

    b. *Demilitarized zone* (DMZ)

5. Name *four* goals of auditing. [2]

6. Recall that we use constraint p: action -> condition. Use this to identify what should be logged for Biba's integrity model (provide formula). Do you strictly need to log subject (S) and object (O)? [4]

7. 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? [2]

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

8. One way to *sanitize* information is to replace each piece of information with random pseudonyms. What would be a problem with that? [2]

9. Enumerate the key *Risk Assessment* steps [3]

10. For the risks and the security mechanism indicated below, calculate and insert the values as per the given data: [4]
    - Risks:
        - disclosure of company confidential information,
        - computation based on incorrect data
    - Cost to correct data: $3,000,000
        - @20% liklihood per year: _____
        - Effectiveness of access control software: 60%: -$60,000
        - Cost of access control software: +$45,000
        - Expected annual costs due to loss and controls: _____
        - Savings: _____

11. Answer *only one* of the following: [3]

    a. Differentiate between spatial domain and frequency domain watermarking.
    b. Write differences among *copyright*, *patent* and *trade secret*.
    c. Briefly explain two tools that are useful for forensic analysis of Computer intrusions.
    (*Provide answer on the back of a sheet*)

Part IV: Malicious code, Vulnerability, Intrusion Detection, Physical Security & Disaster Recovery (25)

1. Define the following terms [2]

   Polymorphic virus:

   Worm:

2. Write in the blank spaces [2]
   i. Two ways of *detecting* viruses are:

      [a] _____

      [b] _____

   ii. Two general ways to *defend* against a virus

      [a] _____

      [b] _____

3. Recall the following example of a Trojan horse [3]

   - *Perpetrator*

     1. cat >/homes/victim1/ls <<eof
     2. cp /bin/sh /tmp/.xxsh
     3. chmod u+s,o+x /tmp/.xxsh
     4. rm ./ls
     5. ls $*
     6. eof

   That is, the perpetrator creates a file called ls in *Victim1*'s home directory

   - *Victim1*
     ls

     That is, when *Victim1* executes the file ls, he will be running a Trojan horse created by the *Perpetrator*.

If *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 needd to be inserted in the script above.

4. Recall the simple virus code: [3]

```
1. BeginVirus
2.     If spread condition then
2.         For target files
3.             if not infected then
                   alter to include virus (lines 1-6)
4.     Perform malicious action
5.     Goto to beginning of the infected program
6. EndVirus
```

   Modify the *pseudo-code* to make it a *stealth* virus

5. What are the steps involved in the Flaw Hypothesis methodology. [2]

6. 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)
```

   a. State what is the cause of the problem with *xterm*.

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

7. NRL taxonomy of software vulnerability includes three schemes. These are: [2]

   1. _____
   2. _____
   3. _____

8. Differentiate between Aslam's *Coding faults* and *Emergent faults*. [2]

   Coding faults

   Emergent faults

9. Write three practical goals of an Intrusion Detection System. [2]

10. What are the two type of Intrusion detection system? Differentiate between them by writing their characteristics. [2]

11. What are *Honeypots*? (2)

12. What is TEMPEST program? Name two ways of protecting against emanations [2]

13. Indicate factors that need to be considered before disposing sensitive media. [2]

14. Identify two natural disasters and factors related to them in terms of protecting information system resources. [2]

15. Indicate two elements that a security plan should address and state what they mean. [2]