

**IS2935 Introduction to Computer Security**  
**Final Examination**  
**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 20)

Part 3: (Total Score 30)

Part 4: (Total Score 30)

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

---

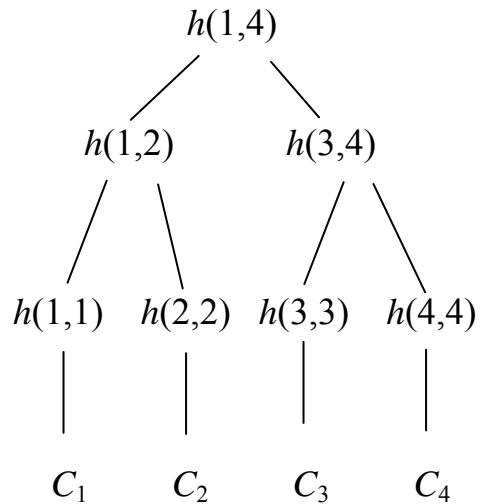
**Score**

Part 1 (20)	Part 2 (20)	Part 3 (30)	Part 4 (30)
Total =			

***Best of Lucks!!***

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

1. Refer to the Merkle'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  $X\langle\langle Y \rangle\rangle$  represents  $Y$ 's certificate signed by  $X$ . Consider the following certificates and answer (a) and (b) below. [2, 2]
  - $Dan\langle\langle Alice \rangle\rangle$
  - $Cathy\langle\langle Bob \rangle\rangle$
  - $Dan\langle\langle Cathy \rangle\rangle$
  - $Cathy\langle\langle Dan \rangle\rangle$

- (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 Bob takes to validate Alice's certificate:
3. What is a *dictionary* attack? Briefly describe the two types of *dictionary* attacks. [4]
4. Provide argument(s) *for* or *against* the following statement: [2]  
“Use of salt increases the effort needed to launch a dictionary attack on passwords.”
5. For the *S/Key* scheme for password authentication, write the following: [2, 2].
- a. If  $h$  is the hash function used,
- (i) the  $n$  keys,  $k_1, k_2, \dots, k_n$  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 the user will use because of the following reason:
6. Identify two *biometric* authentication systems and give examples of attacks on them. [2]  
(Provide answer on the back of the adjacent page)

## Part II: Design Principles, Assurance (Total Score 20)

1. Write what the following *design principles* mean. [6]

*Fail-safe defaults*

*Economy of mechanisms*

*Psychological acceptability*

2. What do you mean by *operational assurance*? State its importance. [2]
3. What are the three required properties of a *reference validation mechanism*? [2]
4. Give two characteristics 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 security evaluation 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  $p_i$ : *action*  $\Rightarrow$  *condition*. Show these constraints and identify what should be logged for a system employing the following Biba's integrity model. Do you strictly need to log subject (S) and object (O)? [4]

Biba's Model: *Strict Integrity Policy*

- $s \mathbf{r} o \Leftrightarrow i(s) \leq i(o)$  (no read-down)
- $s \mathbf{w} o \Leftrightarrow i(o) \leq i(s)$  (no write-up)
- $s_1 \mathbf{x} s_2 \Leftrightarrow i(s_2) \leq i(s_1)$

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% likelihood 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.



## Part IV: Malicious code, Vulnerability, Intrusion Detection, Physical Security & Disaster Recovery (30)

1. Define the following terms [2]

*Polymorphic virus:*

*Worm:*

2. 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*.

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.

3. 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.  
 (Provide your answer on the back of the adjacent page)

4. What are the steps involved in the *Flaw Hypothesis* methodology. [3]
  
5. 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* that we are referring to.
  
- b. Briefly describe why the above check still makes *xterm* vulnerable to “race condition”.
  
6. *NRL taxonomy* of software vulnerability includes three schemes. These are: [2]

a. \_\_\_\_\_

b. \_\_\_\_\_

c. \_\_\_\_\_

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

*Coding faults*

*Emergent faults*

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

9. What are the two types of *intrusion detection* systems? Differentiate between them by writing their characteristics. [4]

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

11. Identify two natural disasters and state how one may protect information system resources against them. [2]

12. Enumerate two key elements that a security plan should address and state what they mean. [2]