EECE 412, Fall 2005

Midterm Examination

Your Family name: _____
Your First name: _____
Your student ID: _____

Name of your left neighbor: _____
Name of your right neighbor: _____

---

1. (3 points) When should access control mechanisms **NOT** be used? Select all applicable.

A. When there is no way to check the rules
B. When there is no trust to enforce the rules
C. When it is possible to enforce and check the rules

Answer: _____

2. (4 points) Which properties are **NOT** required for a good random function? Select all applicable.

A. "one-wayness"
B. invertible
C. collision resistance
D. the key should not be reused

Answers: _____

3. (3 points) Which of the following cryptographic schemes would remain viable even if quantum computing becomes as powerful as some of its advocates speculate (i.e., quantum computers will be able to compute NP-hard and other computationally expensive problems in short time). Select all applicable:

A. Diffie / Hellman
B. RSA
C. One time pads
D. AES

Answers: _____

4. (3 points) Which of the following (select all applicable) conditions a good public key cryptosystems does **not** have to meet?

A. It must be computationally easy to encipher or decipher a message given the appropriate key.
B. It must be computationally infeasible to derive the private key from the public key.
C. It must be computationally infeasible to determine the private key from a chosen plaintext attack.
D. It must be computationally infeasible to derive the public key from the private key.

Answers: _____

5. (5 points) Answer T(RUE) or F(ALSE) to each of the questions below.

[ ]A symmetric cipher is an invertible function.
[ ]The Caesar's cipher is a poly-alphabetic permutation cipher.
[ ]The ECB mode of operation is not recommended for the transmission of long messages.
[ ]In CBC mode, the initialization vector IV is sent as the last block of the cipher-text.
[ ]The DES S-Box implements a permutation.

6. (4 points) In a digital signature scheme, we compute the message digest first and then encrypt the result using the sender's private key: $S = \{H(M)\}_K$. What if the process were reversed: $S = H(\{M \}_K)$? Would it yield the same type of integrity? Explain why or why not.

7. (5 points) Some network security protocols use interchange keys different from session keys. Explain the difference between an interchange key and a session key, and list two reasons why it is important to use both interchange and session keys.

8. (6 points) You are a security analyst for a major bank. Your boss asked you to develop recommendations for countermeasures to the possible threat of IP address spoofing in the bank's intranet. Which of the following countermeasures would you recommend? (select all applicable)

A. DHCP snooping
B. Ingress access list
C. BPDU guard
D. Dynamic ARP inspection
E. IP source guard
F. Port security

Answers: _____

9. (8 points) Explain your rationale for selecting the countermeasures in the previous problem.

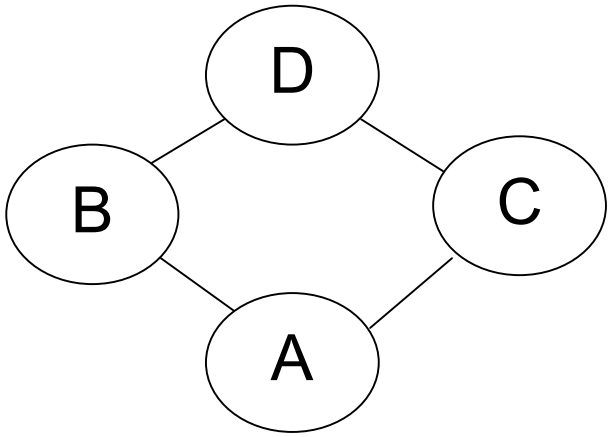
10. (2 points) UBC ECE and CS departments together with ICICS use Access Control Management System (ACMS) that employs Access Key cards a.k.a. key fobs. To unlock a door controlled by ACMS a user presents her key fob to the fob reader, which "reads" the fob's access control ID number. The number is used by the ACMS to determine if the user has the right to unlock the door. The described ACMS is based on

A. Capability lists (c-lists)
B. Access control lists (ACLs)

(select one).

11. (4 points) Explain your answer to the above question:

12. (8 points) For the following BLP lattice



Fill out the psudo-access matrix (follow the example for B):

		Objects			
		A	B	C	D
Subjects	A				
	B		RW		
	C				
	D				

13. (15 points) You are tasked with the security analysis of the following password-based authentication solution for an online banking application to be used primarily with mobile phones. The application is expected to be very popular among college and university students. The user uses his GPRS-capable mobile phone with a limited Web browser-like client application to log into the system by typing or speaking the user name and the password, which are sent over the mobile phone service provider to the bank server. If the user name or password was spoken, it is translated into text using voice recognition software on the server. The server then checks the password against its accounts database and successfully authenticates the user if the check succeeds. The user has to re-authenticate after 20 minutes of inactivity or after login out.

1. Analyze threats and possible vulnerabilities of the above authentication scheme. Explain what can go wrong and why.
2. Suggest reasonable improvements to the scheme.

14. (10 points) You are a system administrator at Small University with Virtual classrooms, which runs all its services on Linux machines. Here's a summary of the worm's work:

1. calls RNG to get a random class B subnet
2. adds the worm startup script to /etc/rc.d/rc.sysinit
3. starts an HTTP server on port 27374
4. patches the exploits that it used for the attack
    a. Kills the process & removes rpc.statsd binaries
    b. Disables anonymous FTP
    c. Uses modified synscan to contact a random IP address and check the FTP banner
       "220 webct.suv.ca FTP server (Version wu-2.6.0(1) …) ready.)"
       to determine if the machine is running Red Hat Linux 6.2 or Red Hat Linux 7.0.
5. Red Hat 6.2: exploits rpc.statd or wuftpd service vulnerability.
6. Red Hat 7.0: exploits LPRng vulnerability.
7. downloads the rest from the attacking machine
8. extracts the contents and executes start.sh
9. sends email message anonymous Yahoo! and Hotmail email account specifying the IP address of the attacked machine.
10. Replaces the content of the host's index.html file at the root of the web server document tree.

Given the above specifics and structure of Ramen Worm, suggest ways of detecting and/or preventing it from successfully attacking SUV IT infrastructure.

15. (15 points) Bonus problem: Draw an RBAC role hierarchy and permission-to-role assignment table that would precisely simulate the BLP lattice from problem 12.