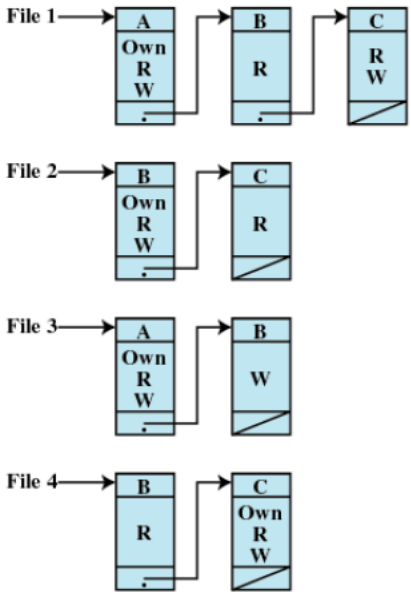
CS 585 – Computer Security
Exam 2
Fall 2021

Make sure there are 7 questions on 8 pages.

Name:_____

1. Convert the following access control matrix into an access control list. (12 points)

	File 1	File 2	File 3	File 4	Account 1	Account 2
User A	Own R W		Own R W		Inquiry Credit	
User B	R	Own R W	W	R	Inquiry Debit	Inquiry Credit
User C	R W	R		Own R W		Inquiry Debit



2. (12 points) Determine whether the following statements are true or false.
Explain your reasons.

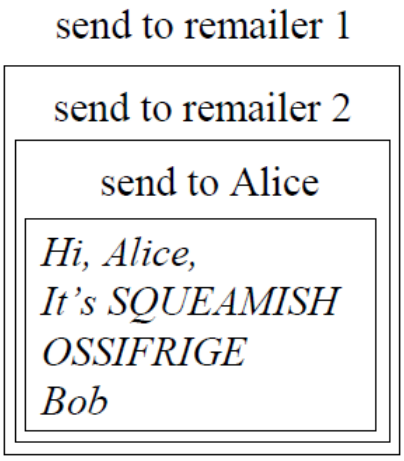
(a) The default permission in Window file system is to deny access. This design principle is known as Fail-safe default.

True.

(b) Clark-Wilson Integrity model
The input data for a deposit (money) into an ATM is a trusted input.

False. Untrusted input.

3. Explain the mechanism of Cypherpunk Remailer. (12 points)



For sender
Encipher message
Add destination header
Add header for remailer n …
Add header for remailer 2

For remailer
Remove header and forward to the next remailer.

4. (10 points).
Organize the following companies into “conflict of interest” classes.
Shell Oil, Standard Oil, Band of America, and Citi Bank.

Two classes:

Shell Oil, Standard Oil

Band of America, and Citi Bank.

5. (18 points)
Given the security levels {TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED} and categories {A, B, and C}. What type of access (read, write, both, or neither) is allowed ? **Why?**

1. Paul cleared for (TOP SECRET, {A,C}), wants to access a document classified (SECRET, {B,C})

   Neither

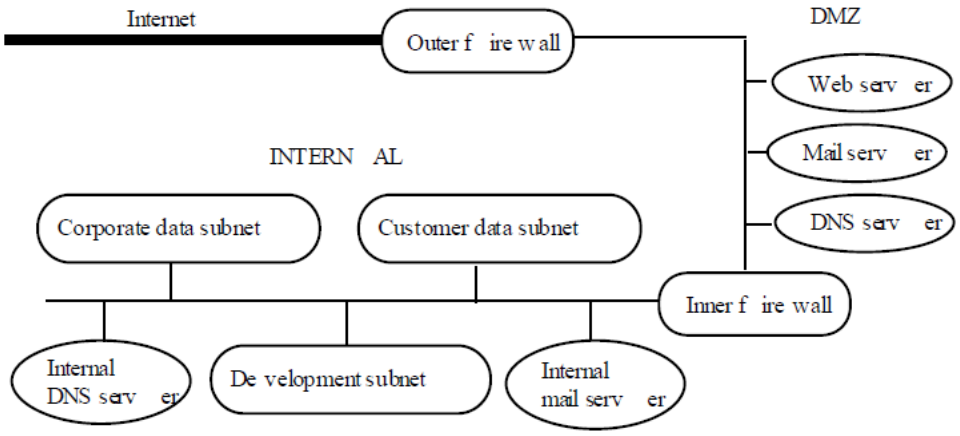
2. Jesse, cleared for (SECRET, {C}), wants to access a document classified (CONFIDENTIAL, {C})

   Read

3. Provide a sample document that Bob, cleared for (Secret, {A, B}), can both read and write.

(Secret, {A, B})

6. (24 points) A typical enterprise network as we discussed in class includes multiple servers, firewalls, and PCs.
(a) Draw a picture to show an enterprise network with DMZ. (12 points)



(b). Suppose that you are a system administrator. What types of network connections will you allow to be established with the servers in the DMZ from the Internet? (6 points)

HTTP,
HTTPS,
SMTP

(c). If the company sales products online, how do you secure the customer data? (6 points)

Encrypt
Download to internal network periodically

7. (12 points) Determine whether the following statements are true or false.
Explain your reasons.

a) Even if the cookie's domain does not match that of a web server, web browser can still send a cookie to the web server.

True.

b) Discretionary Access Control is one type of Authentication.

False. DAC: is access/authorization. It is based on the identity of the requestor and on access rules stating what requestors allowed to do.