Robert Jones

Homework 2 - Access Control

1. Commands for firewall rules

```
// include 172.97.0.0/16 but exclude 172.97.255.0/24 can browse on port 8888

iptables -A INPUT -s 172.97.255.0/24 -p tcp --dport 8888 -j DROP
iptables -A INPUT -s 172.97.0.0/16 -p tcp --dport 8888 -j ACCEPT

// only 172.97.10.20 SSH port = 22 ping = icmp

iptables -A INPUT -s 172.97.10.20 -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -s 172.97.10.20 -p icmp -j ACCEPT

// Server can’t send anything out

iptables -A OUTPUT -j DROP

// Default policy is ACCEPT

iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT

iptables -A OUTPUT -m -state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -m -state --state RELATED,ESTABLISHED -j ACCEPT
```

2. Permission Check Function

```
int accesscheck(unsigned int uid, unsigned int gid, unsigned int p, int f){

   // get permission infromation from file requested
   Permission filePermission = getPermission(f);

   // if user ID and owner ID match check permissions
   if (uid == filePermission.uid){
       // if owners permission matches request operation, grant access to all
permissions
       if(p == filePermission.u) {
           // grant access
           return 1;
       }
   }

   // otherwise if the users group ID matches the group ID check permissions
   else if (gid == filePermission.gid) {
       // if group permission matches request opperation, grant access to all
permissions
       if (p == filePermission.g){
           // grant access
           return 1;
       }
   }

   // otherwise if the user is neither the owner nor in the group of this file,
permissions
   // will be checked agianst the "others" permissions
   else {
       if (p == filePermission.o){
           return 1;
       }
   }

   // access denied
   return 0;
}
```

3. Access Control Matrix

Users/Files	Alice file a	Bob file b	Cyndy file c
Alice	r, w, x	r	-
Bob	r	r, w, x	-
Cyndy	r	r, w	r, w, x

B.) Access Control List and Capability List

Access Control List

1. File a
    - Alice: read, write, execute
    - Bob: read
    - Cyndy: read
2. File b
    - Alice: read
    - Bob: read, write, execute
    - Cyndy: read, write
3. File c
    - Alice: none
    - Bob: none
    - Cyndy: read, write, execute

Capability List

1. Alice
    - File a: read, write, execute
    - File b: read
    - File c: none
2. Bob
    - File a: read
    - File b: read, write, execute
    - FIle c: none
3. Cyndy
    - File a: read
    - FIle b: read, write

- File c: read, write, execute

C.) New ACM

Users/Files	Alice file a	Bob file b	Cyndy file c
Alice	r, w, x	r	r
Bob	-	r, w, x	-
Cyndy	r	r, w	r, w, x

4.) Controlled Policy

a.) Linux

- Policy Type: Discretionary
- Creator: The user who creates the file
- Owner of the object: Owner of the file
- System: Linux
- Admin: owner of the file
- Who decides permission: owner of the file

b.) Software repository

- Policy Type: Originator Controlled
- Creator: Author of the software package
- Owner of the object: The author of the package
- System: Software repository
- Admin: Repository admin, with authors consent
- Who decides permission: The author of the package

c.) Classified NSA database

- Policy Type: Mandatory
- Creator: NSA
- Owner of the object: The U.S. government
- System: NSA classified database
- Admin: Security personnel overseeing the database
- Who decides permission: rules based on top secret clearance

5.) Bell-LaPadula model

a.) Jesse, cleared for (Top secret, {A, C}), wants access to (confidential, {A}

Access = read
Jesse can not write down, she could write to (Top secret,{A}) or (Top secret,{A,C})

b.) Anna, cleared for (Top secret, {A, C}) wants access to (Secret, {B, C})

Access = neither

Anna can read (Secret, {A, C}

Anna can write (Top secret {A, C})

c.) Paul, cleared for (Confidential, {C}) wants access to (Confidential, {B})

Access = neither

Paul can read (Non-classified, {C}

Paul can write (Secret, {C})

d.) Sammi, cleared for (Secret, {C}) want access to (Confidential, {C})

Access: read

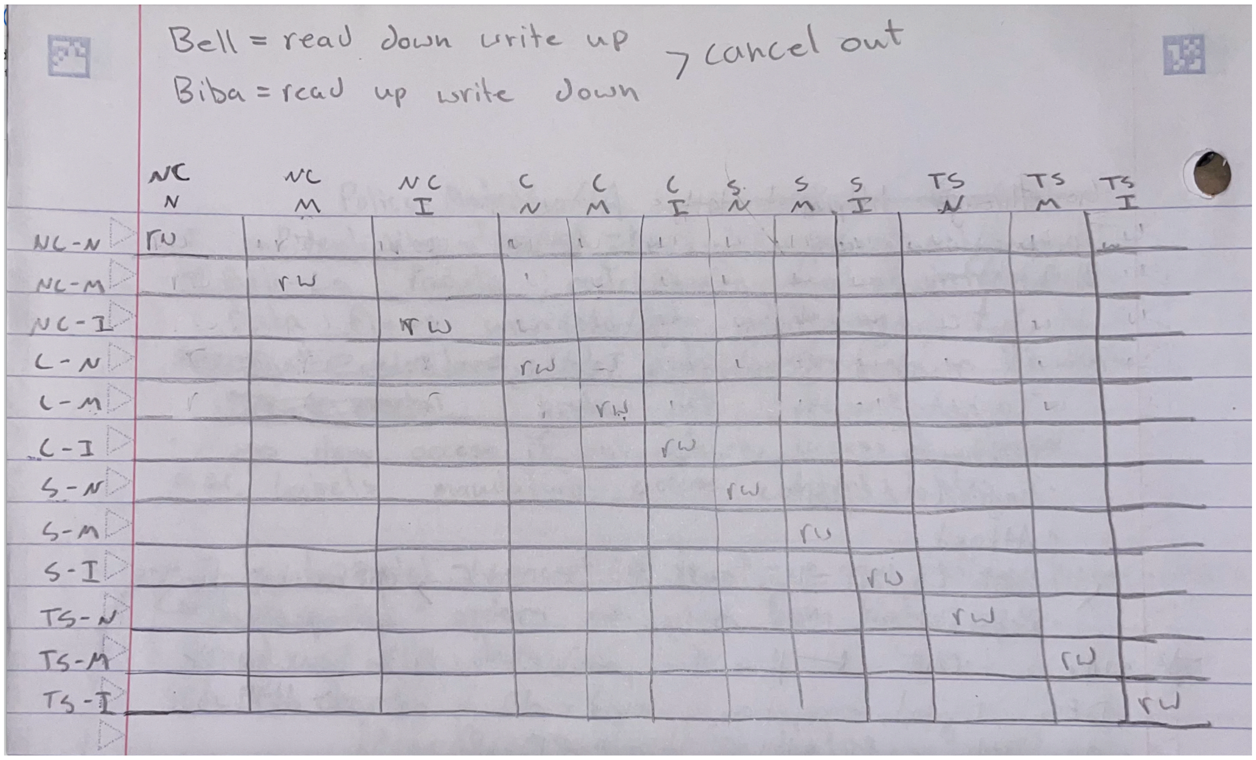
Sammi can write (Top Secret, {C})

e.) Robert has no clearance, (Confidential, {B})

Access: neither

Robert has no clearance in any category, he only has access to Non-classified documents.

6.)



Bell = read down write up

Biba = read up write down

$\Big\}$ cancel out

	NC N	NC M	NC I	C N	C M	C I	S N	S M	S I	TS N	TS M	TS I
NC-N	rw											
NC-M		rw										
NC-I			rw									
C-N				rw								
C-M					rw							
C-I						rw						
S-N							rw					
S-M								rw				
S-I									rw			
TS-N										rw		
TS-M											rw	
TS-I												rw