שאלה 1

		S	TS
		f_1	f_2
C	U_1	W	W
S	U_2	RW	W
TS	U_3	R	RW

א)

$$ACL(f_1) = \{(U_1, W), (U_2, RW), (U_3, R)\}$$

$$ACL(f_2) = \{(U_1, W), (U_2, W), (U_3, RW)\}$$

ב)

$$clist(U_1) = \{(f_1, W), (f_2, W)\}$$

$$clist(U_2) = \{(f_1, RW), (f_2, W)\}$$

$$clist(U_3) = \{(f, R), (f_2, RW)\}$$

ג)

owner של f_1 הוא U_2 ו
owner של f_2 הוא U_3, f_1 ו
U_3 יכול לשנות את f_1, U_2 יכול לשנות את f_2
ו U_1 לא יכול לשנות כלום.

	O	G	O W
f_1	R--	-W-	RW-
f_2	-W-	---	RW-

ג) פונקציות לדוגמה שונות!

ב) מערכות Windows-ים ACL ו-
מערכות!

שאלה 2

א) יהי כיוון חלש. הוכיחו $X = Y$
לכל Z.
לכן הוכיחו קיימת כיוון ℓ כך ש
$\ell(Z) \geq \ell_1 \oplus \ell_2$
בדוגמה $\ell(Z) \geq \max(\ell_1, \ell_2)$

ב) הוכיחו כי!

*

X	Y	Z
0	0	1
0	1	2
1	0	3
1	1	2

$p(z=1) = 1/4$

$p(z=2) = 1/2$

$p(z=3) = 1/4$

$H(X,Y) = 2$

$H(X,Y|Z=1) = 0$

$H(X,Y|Z=3) = 0$

$H(X,Y|Z=2) = \frac{1}{2}\log\frac{1}{2} + \frac{1}{2}\log\frac{1}{2} = 1$

$H(X,Y|Z) = \frac{1}{4}\cdot 0 + \frac{1}{2}\cdot 1 + \frac{1}{4}\cdot 0 = \frac{1}{2}$

שאלה 3

א) (authentication) אין שני הצדדים
השולח יכולה סודית K_s משני.
ב. הפשרות של T היא שני של A
כדי למנוע Replay של הודעה ישנה.
הבעיה היא שהשרת של B (או
DOS אחר) כבוי, ואז ה T של
DOS יהיה גדול ל T של B.
ג. הפתרון ב B שלא שאל שאלה
חדשה שהוא יכול A ו יכול
לפענח את ההודעה K_s ולכן לשלוח את
ההודעה N_1 לשלוח את
$f(N_1)$.

ד. ההבדלים הם שיש לצדדים
אחדות כמו שעון משותף
מסונכרן. היתרונות הם קצר
יותר בהודעות Time Stamps.
כמו כן יש צורך "שמירה"
של Life-time של הנכסים. כמו כן
יש צורך ב Authentication
שלא מאפשר הזיוף ומאשרת את
הנכונות ההודעות של כל צומת.

שאלה 4

"משאבי פחות בטח"

משרד, אבטחה, מחשב הודעה (שפה)
כדי מאפשר מחשב בפנה בתקינות (שפות)
שונות.

כאשר כל שינוי בטבלה יגרור אוטומטית
שינוי בשאילתא המתאימה לטבלה.

הסבירו בקצרה

קונסיסטנטיות מתקיימת, כאשר שאלת ה
שמוחזרת נכונה. נכונות היא יחסית
לשאלה "הנכונה" שרצינו שתוחזר.

הסבירו בקצרה שלמות

קונסיסטנטיות שמתקיימת. כאשר ~~כל~~ ישנם
ערכים חוקיים שמוחזרים בשאילתא
שרצינו שתוחזר.

הסבירו בקצרה שלמות

ישנם כאלה
שמוחזרים כלפי חוץ.
טבלה אחת (שמות) שמקשרת בטבלה
שנייה אחרת (תפקידים) שלישית.

אחזרו מסד נתונים, כך שלפי
אחד נתקיים.

~~בקצרה~~
בקצרה טבלה אחת בשאילתא
שנייה, בקצרה טבלה נוספת. כך שלפי
טבלה הנוספת כל שינוי שיבוצע
על ה DB. בשאילתא טבלה כך שתוחזר
~~שאילתא~~ שאילתא (שאילתא) את שאילתא שתקבלנו
בקצרה מינימום השינויים לפני הפעולה
שלמה הפעולה לא שתבוצע.
שאילתא בשאילתא שמקבלת אנשים ו
כל שאילתא כזאת נשאילתא שלישית!

שאלה 5

א

1) ACL - רשימת הסיסמאות, לכל קובץ הרשאה שלו יש גישה לכל משתמש

2) C-list - משתמש. בניגוד לקודם שם כל הקבצים לכל משתמש

3) קבוצות - שיתוף קבצים בין משתמשים שונים בקבוצה.

4) כל משתמש. יש הרשאות שלו!

ב

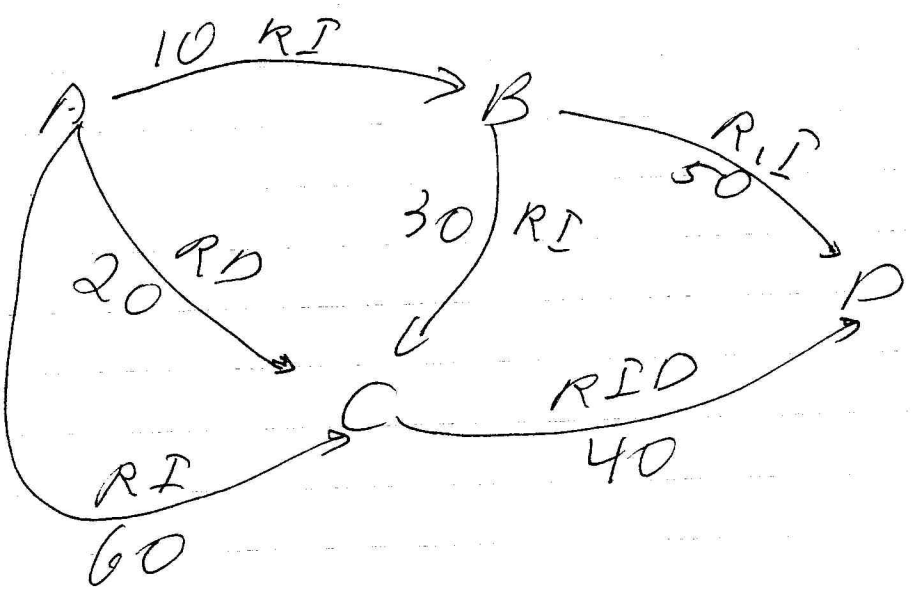
1) ACL - כל
2) C-list - קבוצה משתמש לא שמשנה
3) Unix - שים את Steve ו Mitch בקבוצה ובקבוצה
4) כל

ג

1) ACL - משתמש שיש בניגוד הרשאה שלו.
2) משתמש.
3) כל קובץ הרשאה כמו שיש לשם בקובץ מלא הרשאה
4) כל

שאלה 6

א)



ב)

ב- System R נבדוק הרשאה מסוג I
על B. נבדוק I הרשאה על D.
נבדוק RID הן הרשאות על
אכזרון שהן ניתנו על C בצמן
אחרות.

ב- SQL-92 נבדוק I
הן הרשאה על אכזרון שקיימת
שכולל רשאה לכל פעולה על C.
(בצמן הן הרשאה)