

ארגון ותוכנות המחשב

תרגיל 2 - חלק י Bush

המתרגל האחראי על התרגיל: תומר צץ.

שאלותיכם במידע בעניינים מנהליים בלבד, יופנו רק אליו.

כתבו בתיבת subject: Bush 2 את"ם.

שאלות בעל-פה ייוננו על ידי כל מתרגל.

הוראות הגשה:

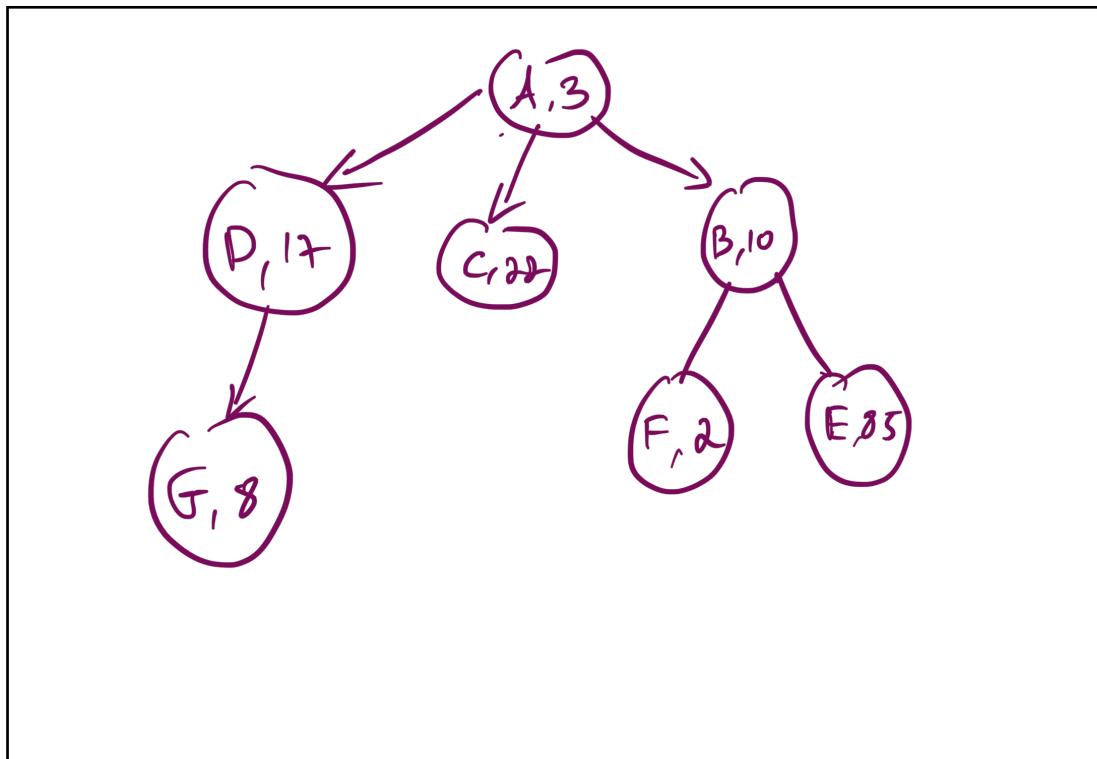
- לכל שאלה יש לרשום את התשובה במקום המועד לכך.
- יש לענות על גבי טופס התרגיל ולהגיש אותו באתר הקורס כקובץ PDF.
- על כל יום איחור או חלק ממנו, שאינו בתיום עם המתרגל האחראי על התרגיל, יורדו 5 נקודות.
- הגשתה באיחור יש לשלווה למיל של אחראי התרגיל בצירוף פרטים מלאים של המציגים (שם+ת.ז.).
- שאלות הנוגעות לתרגיל יש לשאול דרך הפיאצה בלבד.
- ההגשה בזוגות.

שאלה 1 (45 נק') – שגרות:

נעה המ"מ שמעה כי היא הולכת לקבל מוחזר עתודאים. נעה לא יודעת מה עושים העתודאים בזמןם בחופשי אז היא החיליטה לרשום להם תוכנית באסמבלי לשעות הפנא. לפניכם מקטע הנתונים שנעה כתבה:

1	.section .data	16	E: .long 85
2	A: .long 3	17	.quad 0
3	.quad B	18	F: .long 2
4	.quad C	19	.quad 0
5	.quad D	20	G: .long 8
6	.quad 0	21	.quad 0
7	B: .long 10	22	
8	.quad E		
9	.quad F		
10	.quad 0		
11	C: .long 22		
12	.quad 0		
13	D: .long 17		
14	.quad G		
15	.quad 0		

- א. ציירו את הגרף המתkeletal מפירוש מקטע הנתונים (מומלץ להסתכל בתרגיל 3 תרגיל 1 ולהזכיר כיצד מפרשים את הדיזכרון כרשימה מקושרת). בכל צומת בגרף צינו את התווית המתאימה לו בלבד (אין צורך לציין ערכים נוספים) (3 נקודות)



הסמלת ספייר, שבאה לעזור לנויה, חשבה איך לשעשע את העתודאים הצעירים. לצורך כך, היא כתבה את הפונקציה הפשוטה `func` וקוד שמשתמש בא:

```

23   .section .text
24   .global _satart
25   _start:
26       mov $17, %esi
27       mov $A, %rdi
28       call func
29       movq $1, %rdi
30       sub %rax, %rdi
31       movq $60, %rax
32       syscall
33
34   func:
35       push %rbp
36       movq %rsp, %rbp
37       cmpl %esi, (%rdi)
38       jne next
39       mov $1, %rax
40       jmp end
41
42   next:
43       mov $0, %r10
44   test:
45       cmpq $0, 4(%rdi,%r10,8)
46       je fail
47       push %rdi
48       push %r10
49       mov 4(%rdi,%r10,8), %rdi
50       call func
51       pop %r10
52       pop %rdi
53       cmpq $0, %rax
54       jne finish
55       inc %r10
56       jmp test
57
58   finish:
59       mov $1, %rax
60       jmp end
61
62   fail:
63       mov $0, %rax
64   end:
65       leave
66       ret
67

```

ב. נתון שבתחילת התוכנית ערך של `rsp` הוא `X`. כאשר `X` הוא מספר הקסדצימלי. מה הוא הערך המקסימלי ומה הערך המינימלי ש-`rsp` יכול לארוך ריצת התוכנית? הבינו את התוצאה באמצעות נוסחה שהמספרים בה הם בסיס הקסדצימלי (בטאו את התשובה באמצעות `X`). (7 נקודות)

$$X - 56 \leq RSP \leq X$$



ג. רשמו מה יהיה פלט הפונקציה עבור קטע הקוד הנוכחי (5 נקודות).

ד. המירו את הפונקציה לשפת C על ידי כך שתשלימו את המקומות החסרים בקוד. היעזרו בהגדרת `struct` שנתונה לכם (10 נקודות):

```

typedef struct _Node{
    int data;
    struct _Node** sons;
}Node;

```

הערות:

1. מבנה `struct` בזיכרון אליו היו היבטים מקומליים את הקוד היה שונה מהצורה שבו הוא מופיע בקטע `data` לעיל. הסיבה טוביה לכך שתשילמו ל�ם בהערה הבאה.
2. הניחו שהכוונה ב`**Node` היא שרשימת המצביעים לבנים נמצאת בתוך `struct` ומוצגת כמערך באורך לא קבוע (ולכן גם `struct` בגודל לא קבוע). דבר זה אינו חוקי בשפת C. שפה C תופס מקום קבוע בזיכרון. לשם התרגיל אנחנו מניחים שהוא חוקי, שניתן להשיג רק בזכות העבודה שאנו כותבים באסמבלי)
3. מותר להשלים יותר ממילה אחת בכל קוו אך לא יותר מפוקודה אחת!

```

bool func ( Node *root, int x){
    if (root->data == X)
        return True;
    Node *son = root->sons;
    while(son != null) {
        if (func(son, x))
            return True;
        son += 1.
    }
    return False;
}

```

הערה: בסעיפים הבאים יש כל מיני שינויים בקוד. כל שינוי מתקיים רק בסעיף בו מופיע. זאת אומרת שהסעיפים לא תלויים אחד בשני.

ה. ציליל המ"כית מאמינה שהכל צריך להיות אחיד ומסודר. היא מחליטה לחת את מקטע הנתונים של נועה ולשנות בכל struct את הוגו longoa בquad. כמוום מקטע הנתונים ישתנה כך:

```

1 .section .data
2 A: .quad 3
3 .quad B
4 .quad C
5 .quad D
6 .quad 0
7 B: .quad 10
8 .quad E
9 .quad F
10 .quad 0

```

ובאופן דומה כל שאר האותיות יחליפו את הנתון הראשוני במקומם בquad. רשמו את השינויים שצריכים להיות בקוד על מנת שייעבוד בצורה תקינה עם מקטע הנתונים החדש

(5 נקודות)

4(.rdi, r108) קראם 8(.rdi, r108) - 45,49
cmpd פתקן empq, 37 ר7
esi פתקן fsi - ג לינ'ל

- ו). יוגב הסמ"ץ אוחב לעזר לנועה ולן החליט לשנות את מבנה הנתונים באופן הבא:

```
13    D: .long 17
14          .quad A
15          .quad 0
```

- מה יהיה פלט התוכנית? יש לסמן תשובה מבין התשובות הבאות ולנמק במשפט אחד: (5 נקודות)

 - a. התוכנית תסתה ופלט הפונקציה יהיה 1
 - b. **התוכנית תסתה ופלט הפונקציה יהיה 0.**
 - c. התוכנית תכנס לוולאה אונסופית
 - d. התוכנית תקרוס במהלך ריצה
 - e. התוכנית כל לא תבנה

$$rdi = 1 - rax = 1 - 1 = 0$$

בימוק: גן של פלטפורם אחד או יותר, מוקם בפונקציית קיון, א-קיון, או קיון.

- ז. הקוד הגיע למב"סית ובגאל קוואר הזמן שלא היה החלטה ל��ר את הקוד. לפניכם מספר שינוי שהמבחן"סית הציעה. עליכם לכתוב עבור כל אחת מההצעות האם נכונות השגרה תיפגע (האם יש קלט עבורו השגרה לאחר השינוי שוניה מהשגרה לפני השינוי). הסבירו בקצרה את תשובהכם!: (10 נקודות)

מחיקת הפיקוד push וpop שבשורות 52 ו-47. קדימה ב-100 שורות נוספת ו-100 שורות נוספת. כרגע מושך פיקודים יתבצע נסיעה מ-push ל-pop. מושך פיקודים יתבצע נסעה מ-pop ל-push.

- b. מחיקת הפוקודה `pop` בשורה 51
הכיתם אפסינו את ה-`IS_CIN` כמפורט בסעיפים 5.1 ו-5.2, אך ה-`pop`
היה מושך ב-`IS_CIN` (3.1.8).

הוספה פקודה push %rdi אחרי test בשורה 44

- d. הוספה הפקודה `push %rdi` אחרי `test` בשורה 44, הוספה הפקודה: `mov (%rsp), %rdi` לפני `cmp` בשורה 56.

שאלה 2 (30 נק') – קריאות מערכת:

ג'ואי מרגיש מתוכסכל מכך שחבריו חושבים שהוא פחות חכם מהם. לכן, הוא מחליט להרשים אותם בעצרת כתיבת קוד באסמבלי. הקוד שג'ואי מתכוון לכתוב קוד שיקרא קלט מהמשתמש שבו הוא יתאר אילו מאכלים הוא מעוניין לקבל והקוד יחזיר לו מה ג'ואי מוכן לתת לו.

- א. לפניים מקטע הנתונים שגואי כתוב מבלי ערכי הנתונים עצם:

```
.section .data
msg1: .ascii ???????
msg2: .ascii ???????
msg1_len: .quad _MSG2 - MSG1
msg2_len: .quad _MSG1_LEN - MSG2
all_msg_len: .quad _MSG1_LEN - MSG1
```

ג'ואי לא יודע עדין אילו מחרוזות הוא יכתוב. עליים להשלים את המקומות הריקים שקשרים לאורכי המחרוזות כך שמשתנה `len` msg1 יהיה האורך של `msg1`, ב`len2` msg2 יהיה האורך של `msg2` ומשתנה `len_all` יהיה שווה לסכום אורכי המחרוזות `msg1` `msg2` ו- `msg3`. שימו לב עליים לעשות זאת בצורה כזו שהאורכים יהיו נכונים בעת ריצת התוכנית ללא קשר לאילו מחרוזות ג'ואי אתה כלערכיהם של `msg1` ו- `msg2`.

- ב. לפני ביצוע קריית מערכת מתבצעים גיבויים של ערכים מסוימים בתוכנית. נרצה להבדיל בין הארכיטוֹרֶת של מערכת המעבד וארכיטוֹרֶת של קוד המשמש. בביטויים גיבויים אלו.

ה- מה באחריות קוד המשפט לగבות?

a. מה באחריות קוד המשמש לגבוי?

כליוגרם \times , r_{ex} , ו- ln ($\text{אפקט רם גלאין מונטגנו}$ כ- המ גלאין אפקט)
וכן ד- רכס נייר

b. מה באחריות מערכת ההפעה לגבוט?

ט. מה באחריות מערכת ההפצה לגבי?

c. מה באחריות המעבד לגבוט?

c. מה באחריות המעבד לגבי הפקודת `encls` ?
הפקודה `encls` מפעילה הפקודה `encl` בזיכרון.

ג'. ג' או רצה לחסוך בזיכרון והעדיף שבסמך למשתמש בsyscall הוא יקרא שירות לפונקציות sys_read ו sys_write שמערכת הפעלה ממסת (יבצע את הפוקודה sys_write call לדוגמה). האם קרייה ישירה כזו תעבוד? אם כן הסבירו לנו מה נדרש לעשות כדי שהזה יעבד והוא יש בכר סיכון. אם לא,

רשמו באיזה אחד משלבי התוכנית (קמפוס, ריצה, טעינה, קישור וכו') יקרה הכישלון ומדובר.

ד. חברה טובה של ג'ואי, פיבי, טוענת שאין בכלל צורך בשתי פקודות `return` שונות. ואמרה לג'ואי לבטל ~~לחולוטין את פקודת sysret~~ ולהשתמש רק ב-`ret`. האם הצעה של פיבי טובה וישראל?

~~R11 → RELAGSI RCX → REP JC PCI
(2SF IC > NIC Wrapper → 2860)~~

רוא שמע על הקוד שג'ואי כותב לו ורוצה להציגו לחגיגה. הוא נסע לכנס מערכות הפעלה השנהית וביקש אישור להוציא קריאת מערכת חדשה `pivot_sys`. קריית המערכת זו תיצור 3 תיקיות עם השם `pivot1`, `pivot2`, `pivot3` (הרשאות התיקייה לא משתנות). האם הקוד של רוא (שיקרא על ידי `entry_syscall` כמו כל קריאת מערכת) צריך לשמור על קונבנציות `V ?system` נמקו.

הסבירו מה על רוס לעשות/להוציא/לשנות לקוד מערכת הפעלה על מנת שהקראה שלו תעבוד (רק לפי מה שלמדתם בקורס)

לפי מה שלמדתם בקורסו
הופכת נפקד ד'הו. syscall נקרא כמו sys_fstat.
הנפקד יתבצע ביכולתו של ה-OS לארון
ה-Handler. והוסה ה-Handler לפונקציה.
כך ה-Processor יזעיק.

גונטר, מנהל בית הקפה, שמע על כל המשחקים במערכת הפעלה שהחברים עושים וביקש מהם לכתוב עבורו גם קריית מערכת חדשה. הוא מעוניין בקריאת מערכת בשם `coffee_order`. היא תקבל בתוך קלט את הארגומנטים הבאים: סוג קפה (מספר שלם), גודל כוס (תו), ליחת אן לשבות (bool), חם או קר (bool), שם המזמין (מחרוזת), האם להוסיף מאפה (bool), האם התשלום באשריאנו במזומנים (bool).

ומחזירה את מספר ההזמנה בתור פلت.
האם ניתן להוסיף קריית מערכת שצוי? נמקו.

הkernel מושך אליו כל הלקוחות ופונקציית kernel_map מושכת מלקוחות אלו לkernel.

שאלה 3 (25 נק') – רמות הרשותה ואוגר הדגלים:

הפקודה `pushfq` דוחفت את הערך של אוגר הדגלים למחסנית. והפקודה `popf` מוציא את אוגר הדגלים מהמחסנית. הסבירו כיצד באמצעות שילוב של שתי פקודות אלו ניתן להציג את הדגלים `OF` ו-`CF`. שימושם ב민ידת אחד הדגלים כבר דלוק יש להשאירו דלוק כלומר, בסיום התהליך על שני הדגלים להיות דלוקים. אין לשנות את שאר הביטים בריגיסטר הדגלים. בנוסף, אין לשנות אף רגיסטר שהוא לא `rflags`, `rip`, `rsp` (גם לא באופן זמני).

הערה: במידת ובדקתם את עצמכם באמצעות דיבאגר וראיתם שנדרך גם דגל TF זה בסדר תלמודו

במהשך מדוע הוא נדליך תורן כדי דיבוג.
 הפונקציית `main` מקבלת אינט (int) ומחזירה אינט (int).
 הפונקציית `sum` מקבלת אינט (int) ומחזירה אינט (int).

RFlags NC NW
AL DSZ. NZC גודל אוניברסיטאי
sf פ' -NSZ, DS RFlags

ב. הול' התחמנית רוצה לאפשר לעצמה גישה ישירה אל התקני הקולט פلت ללא צורך בקריאה
מערכת. איזה שינוי באוגר הדגלים יכול לעזור להול' במטרתה?

הערה: לא צריך לציין פקודה ספציפית. רק להגיד מה צריך לעשות במסגרת התיאוריתית

לנ"ט ינ"ג. ס"כ מונט, הילמן, ס"כ. 2 מיל' כהן גורי.

ג. הול' מחליטה לנסוט את התעלול מסעיף א' רק שבמוקם לשנות את CF וOF היא רוצה לשנות את LOPL. להפתעתה, היא לא מצליחה לשנות את הביטים הללו. הסבירו מה ההיגיון בכך שהיא לא מצליחה לשנות את LOPL? התיחסו לצורך בקיאות מערכת.

לט"מ טרנסFORMER מודולר גיבריל ג'רמיי נאומן, סטודנט תואר ראשון במדעי המחשב וטכניון, ירושלים, ישראל

ד. הול' לא מתייחסת ומנסה לgesht בלעה באופן אחר. היא תכתב עצמה קריית מערכת שתיעזר לה. הקרייה תאפשר לכל משתמש לקרוא לה ולאחר שהיא תסתהם המשתמש יוכל לgesht ישירות להתקני היקלט פטל ללא צורך בקריית מערכת. הסבירו מה על הול' לעשות בקריית

מערכת שהיא כתובת על מנת שהתוכנית שלה תציג.

הפעלה `syscall` מוחזקת בזיכרון כפונקציית גלובלייה. הפעלה מוחזקת בזיכרון כפונקציית גלובלייה.

הערה: הסעיפים הבאים קשורים לפסיקות מומלץ לענות עליהם לאחר תרגול 6.

ה. וויל החבר המבולבל של הווי מתלבט כיצד ניתן לחסום פסיקות תוכנה لكن הוא שואל את הווי.
אילו מבין התשובות הבאות על הווי לענות לו? יש לסמן את האפשרות הנכונה.

1. כיבוי דגל IF באוגר הדגלים
2. הדלקת דגל IF באוגר הדגלים
3. שינוי CPL ל00
4. לא ניתן לחסום פסיקות תוכנה.

ו. כתעת נתון שווי הצליח להגיע למצב שבו CPL שווה ל0. וויל מעוניין לחסום פסיקות חומרה שאין מועברות דרך כניסה NMI. כיצד הוא יכול לעשות זאת? (5 נקודות)

1. כיבוי דגל IF באוגר הדגלים
2. הדלקת דגל IF באוגר הדגלים
3. עליו לחבר את הפסיקות לכנית NMI ואז לכבות את דגל IF
4. לא ניתן לחסום פסיקות חומרה ולכן לא יצליח.