תרגיל בית 1 בהנדסה לאחור

236653

סמסטר חורף תשע"ז

הגשה בזוגות עד 16.11.2016 שעה 23:00

חלק א' – התקנת תוכנות – לא להגשה

במהלך הקורס נשתמש במספר רב של תוכנות ומומלץ להתקין אותם מראש:

Visual-Studio - ניתן להוריד גרסת Express חינמית מאתר Microsoft (מתאים לדרישות הקורס) או לחלופין לקבל גרסה מלאה עם רישיון דרך ה-MSDN
(ניתן להיכנס דרך https://csms.cs.technion.ac.il:4423).
ניתן גם להשתמש בגרסה שמותקנת בחווה.

GCC - ניתן להתקין במחשב שלכם (על לינוקס או Windows) או להשתמש במחשבי הלינוקס בחוות המחשבים. שימו לב שה-GCC שאתם מתקינים צריך לתמוך בקימפול ל-32 ביט.

IDA free - ניתן להוריד מ:
https://www.hex-rays.com/products/ida/support/download_freeware.shtml

Immunity Debugger - ניתן להוריד מ:
http://debugger.immunityinc.com

- ניתן להשתמש ב-OllyDbg אם Immunity Debugger לא עובד לכם, קישור להורדה יפורסם בהמשך הקורס.

VMWare - ניתן להוריד גרסה חינמית "VMware Player" (מתאים לדרישות הקורס) או גרסה מלאה דרך ה-VMware store שזמין גם כן דרך https://csms.cs.technion.ac.il:4423.

Windows 7 32/64bit - ISO של Windows 7 כדי להתקין על ה- VMware. ניתן להוריד דרך ה-MSDN.

חלק ב' – היכרות ראשונית – איך נראה קוד C מהודר באסמבלי (להגשה)

נרצה לראות כיצד Visual Studio ו-GCC ממירים קטעי קוד שונים לאסמבלי. לתרגיל מצורף קוד בקובץ ex1.c הכולל מספר פונקציות ב-C, כל אחת מבצעת פקודה או סדרת פקודות, שאנו מעוניינים לדעת איך הן מהודרות. למשל פקודת for או if-then-else. הידרנו את הקוד 3 פעמים ובכל אחת מהפעמים הגדרנו למהדר לייצר קובץ ליווח אסמבלי. הידרנו עם:

1. מהדר Visual C ללא אופטימיזציה.
   מצורף קובץ ליווח בשם noopt.asm.
2. מהדר Visual C עם אופטימיזציה.
   מצורף קובץ ליווח בשם opt.asm.
3. מהדר GCC ללא אופטימיזציה (זו ברירת המחדל).
   מצורף קובץ ליווח בשם ex1.s.

לכל אחת מהפונקציות נתחו את סדרת פקודות האסמבלי שנוצרו, והסבירו בכמה שורות איזה קוד יוצרים המהדרים ומה ההבדלים בין שלושת התוצאות.

שימו לב: הוספנו זוג פקודות nop בתחילת וסוף כל פונקציה כדי להקל עליכם לזהות את מיקומי הקוד שנוצר. אתם מתבקשים להתייחס רק לקוד שנמצא בין זוג ה-nopים הראשונים לבאים. ה-nop-ים נוצרים על ידי קריאה למקרו TWONOPS שמצידו מבקש מהמהדר לייצר פקודות אסמבלי. כפי שתראו, פעולה זו שונה בין מהדרים שונים, ולכן הכנסנו את הגדרתה ל-ifdef שמזהה איזה מהדר בשימוש.

חלק ג' – המשך היכרות ראשונית

כתבו תוכנית C קצרה בשם passwd.c המקבלת קלט מן המשתמש ובודקת האם הקלט זהה לשרשור השמות הפרטיים שלכם. אם הקלט זהה התוכנית תדפיס "OK", אחרת "Wrong ID".
לדוגמה: אם השמות שלכם הם יוסי ודני אז הקלט יהיה yossidanny (בחרו את אחד משני הסדרים האפשריים) ורק עבור קלט זה התוכנית תדפיס "OK".

את הקוד עליכם לקמפל ב-GCC ולוודא שהוא תקין. בנוסף עליכם לייצר קובץ ליווח אסמבלי בעזרת GCC (ראו נספח בעמוד הבא).

נתחו את פקודות האסמבלי שנוצרו, והסבירו בכמה שורות איזה קוד יצר המהדר.

חלק ד' – First Crackme

לתרגיל מצורף קוד אסמבלי crackme.s. נתחו את הקוד וענו על השאלות הבאות:
1. מה תפקידו של המשתנה [esp+284]?
2. מה תפקידו של המשתנה [esp+280]?
3. אילו תנאים ה-Serial Key צריך לקיים כך שיודפס עבורו "Good Job"?

אופן ההגשה:

1. תשובתכם לתרגיל צריכה להיות מוקלדת במחשב ומומרת לקובץ PDF.
2. יש להגיש לתא הקורס הדפסה של תשובתכם, כולל הדפסת הקוד שכתבתם בחלק ג' (passwd.c) וגם הדפסה של קובץ הליווח (passwd.s).
3. יש להגיש אלקטרונית את הקבצים הבאים מכווצים לקובץ zip (ולא שום סוג כיווץ אחר):

passwd.c – הקוד שכתבתם בחלק ג'.

passwd.s - ליווח (קובץ אסמבלי) של הקוד שכתבתם בחלק ג'.

ex1.pdf – קובץ התשובות שהדפסתם בגרסת PDF (לא במקום הגשה בתאים). הקובץ נועד למטרות גיבוי בלבד – מה שייבדק בפועל זה מה שהוגש בתא הקורס.

נספח – הוראות כיצד לייצר קבצי ליווח

שימו לב שעבור חלק ב' אינכם נדרשים לייצר את הקבצים בעצמכם, אלא להשתמש בקבצים שסיפקנו לכם.

Visual-Studio

יצירת פרויקט חדש:

New Project -> Visual C++ -> Win32 Console Application -> Empty Project

הוסיפו את הקוד לפרויקט והעבירו את הפרויקט למצב Release במקום Debug (יש אפשרות בסרגל כלים למעלה). הקימפול צריך להתבצע במצב Release.

ביטול אופטימיזציה:

Project -> Properties -> C/C++ -> Optimization - > Disabled

כדי להחזיר את האופטימיזציה, נבצע

Project -> Properties -> C/C++ -> Optimization - > Maximize Speed

יצירת קובץ ליווח אסמבלי:

Project -> Properties -> C/C++ -> Output Files - > Assembler Output -> Assembly with source code.

הקובץ ייווצר בתיקייה של הפרויקט בסיומת asm או cod.

מומלץ לבטל את ה-Security על מנת ליצור קוד אסמבלי פשוט:

Project -> Properties -> C/C++ -> Code Generation -> Security Check - > No

(נדבר בהמשך הקורס על Security)

GCC

על מנת ליצור קובץ ליווח אסמבלי, נריץ את GCC בצורה הבאה:

```
gcc  -m32  -S  -masm=intel  -fno-stack-protector  passwd.c
```

-m32 קימפול במצב 32 ביט.

-S תרגום לאסמבלי.

-masm=intel - תרגום לאסמבלי בפורמט אינטל.

-fno-stack-protector – ביטול ה-security.

הקובץ ייווצר בשם passwd.s.

שימו לב שעל מחשב 64 ביט יתכן שה-GCC הותקן לכם רק בגרסת 64 ביט (ולכן תקבלו שגיאה בקימפול), אם כך התקינו את ההרחבה ל-32 ביט. בחוה ובמעבדה יש תמיכה ב-32 ביט.