

**עבודת גמר 5 יח"ל**

**נושא העבודה:** Process and Threads Monitor

**שם התלמידה:** הילה רהימפור

**תעודת זהות:** 327075511

**שם בית הספר ועיר:** קריית החינוך ע"ש עמוס דה-שליט, רחובות

**שם המנחה:** ערן בינט

**מועד הגשה:** 24.11.2022

Table of Contents

1. מבוא
   1. נושא העבודה

נושא העבודה שלי הוא תוכנה המאפשרת דיווח ומעקב אחרי תהליכים ותהליכונים הרצים במחשב. התוכנה תציג את התהליכים והתהליכונים השונים ותציג את המשאבים השונים בהם כל תהליך משתמש כמו סוגי זיכרון שונים, נתוני מעבד (CPU) ותקשורת. כמו כן, התוכנה תציג את הסוקטים (sockets) השונים ואת צינורות עיבוד הנתונים (pipelines).

המערכת תאפשר שליטה על תהליכים. כלומר, היא תאפשר ליצור תהליכים ולסגור תהליכים רצים. כמו כן, המערכת שואפת לקחת את המידע אודות הפעילות של המחשב ולבדוק דברים חריגים היכולים להעיד על פרצות מסוימות ולהתריע על מידע מדאיג. המערכת תרוץ על מחשב בודד ותציג באופן גרפי את המידע השונה עם שימוש ב-winforms.

* 1. מטרות מרכזיות

המטרות העסקיות המרכזיות שברצוני להשיג הן:

* הנגשת המידע הקיים על תהליכים ותהליכונים שונים במחשב עבור האדם הפשוט
* שימוש בגרפיקה נוחה ולא מסובכת למשתמש ותצוגה ברורה לעין
* העמקה בנושא התהליכונים במחשב ושילוב מידע על תקשורת (sockets and pipelines)

המטרות האישיות המרכזיות שברצוני להשיג הן:

* העמקה בתחום של מערכות הפעלה- הבנה של מהו תהליך ומהו תהליכון ומה מאפיין כל אחד מהם. כיצד כל תהליכ/ון פועל במחשב ועוד.
* התמקצעות ביצירת גרפיקה עם שימוש ב-winforms על מנת ליצור תוצר מרשים ונוח למשתמש מבחינה גרפית.
* זיהוי של התקפות היכולות להגיע לידי ביטוי בתהליכים שרצים במחשב.
* יצירת עבודת גמר ברמה גבוהה שתשקף את היכולות שלי שבה ארגיש שאני ממצה את יכולותיי
* עמידה בלוח זמנים ויצירת פרויקט מרשים וברמה גבוהה.
  1. רציונל

המוטיבציה שלי לפיתוח הפרויקט היא ליצור כלי שהוא ידידותי לאדם הפשוט שיאפשר לו לדעת ולזהות מה קורה במחשב שלו. בנוסף, אני רוצה ליצור בקרב האדם הפשוט הבנה רחבה יותר במושגים השונים בהם עוסק הפרויקט שלי למשל: CPU, תהליך הרץ במחשב, תהליכונים הרצים במחשב, sockets ועוד.

כמו כן, המוטיבציה שלי באה ממקום אישי. הידע שלי בנושא עליו אני עושה את הפרויקט הוא נמוך אך הנושא מאוד מעניין אותי ולכן יש לי מוטיבציה ליצור תוצר ברמה גבוהה שמעניין אותי ותוצר משופר לעומת התוצרים הקיימים בשוק. אני יכולה להגיד באופן אישי שכאשר את משתמשת ב-Task Manager שהוא תוצר הקיים בשוק אותו אני שואפת לשפר בפרויקט זה, אני לפעמים נתקלת בתסכול מבחינת מספר סיבות ביניהן תצוגה גרפית קופצת ומציקה, חוסר הבנה של המושגים המוצגים, חוסר מידע שמוצג למשתמש ועוד.

בעזרת פרויקט זה אני שואפת להגיע לידע ברמה גבוהה יותר בנוגע למה שקורה במחשב של כל אחד מאיתנו, לידע בנוגע לעיצוב גרפיקה ברמה גבוהה, אסתטית ויפה ולצבור ניסיון בכל הקשור ביצירת פרויקט בעל סדר גודל כזה. כמו כן, אני שואפת ללמוד לעמוד בלוח זמנים ולנהל את הזמן שלי כמו שצריך.

* 1. קישור לחומר הנלמד

הפרויקט שלי מתקשר לחומר הנלמד במספר תחומים.

ראשית, הוא מתקשר לחומר הנלמד על ידי כך שבמהלך השנה (כיתה י"ב) אנחנו לומדים על מערכות הפעלה ומבינים לעומק את המושגים תהליך, תהליכון, CPU ועוד. כמו כן, אנחנו מבינים יותר לעומק כיצד המחשב פועל וזה מה שאני שואפת ללמוד במהלך העבודה על הפרויקט. בנוסף, בשנה שעברה למדנו על המושגים socket ו-pipeline כך שגם זה מתקשר לחומר הנלמד.

בנוסף, במהלך השנה למדנו כיצד לעבוד עם winforms כך שהפרויקט שלי מתקשר גם לתחום הגרפיקה אותו אנו לומדים. כמובן שיש צורך לחקור על הנושא טיפה מעבר לחומר הנלמד.

1. תיאוריה

2.1 תיאוריה

הפרויקט עוסק בתהליכים ותהליכונים הרצים במערכת ההפעלה ווינדוס.

2.2 מוצרים קיימים

כיום בשוק ישנן 2 מערכות הדומות למערכת שלי. הראשונה היא Task Manager והשנייה היא Process Explorer.

Task Manager היא תוכנה מובנת בתוך המערכות של ווינדוס שמציגה את התהליכים השונים ואת הצריכה השונה שלהם. התוכנה מציגה את ה-ID של התהליך, שם התהליך, צריכת ה-CPU, זיכרון מסוג private working set, נתוני תקשורת, צריכת חשמל וסטטוס התהליך (אם הוא רץ, בהמתנה וכו'). כמו כן, התוכנה מציגה את הנתונים כגון צריכת ה-CPU בצורה גרפית באופן כללי לכל התהליכים שם היא מציגה את מספר התהליכים והתהליכונים הקיים במערכת, כמות ה-cores שיש למעבד, ה-socket השונים ועוד. בנוסף, היא מאפשרת לעצור וליצור תהליכים.

Process Explorer היא תוכנה חופשית שמותאמת עבור מערכות הפעלה מסוג ווינדוס והיא לא דורשת התקנה. ניתן להגדיר אותה כתוכנת ברירת מחדל במקום Task Manager. בדומה ל-Task Manager, גם Explorer מציגה את התהליכים השונים ואת הצריכה של כל תהליך אך היא עושה זאת בצורה מעמיקה יותר. התוכנה מסוגלת להציג גם את התהליכונים השונים ואת הצריכה שלהם, מה ש-Manager לא מסוגלת לעשות. היא מציגה את ה-ID של התהליכון, מצב התהליכון, המעבד האידיאלי עליו רץ התהליכון, ההעדפה של התהליכון ועוד. גם מבחינת תהליכים, Explorer מציגה נתונים מעמיקים יותר. היא מציגה יותר סוגי זיכרון שהתהליכים צורכים (למשל, woking set private, working set shared, peak working set ועוד). כמו כן, התוכנה מציגה בצורה גרפית את הצריכה של כל תהליך (בניגוד ל-Manager שמציג באופן כללי את הצריכה). כמו כן, התוכנה מאפשרת חיפוש, סינון ופילטרים שונים ותצורתה הגרפית מאוד נוחה לעין מה שמקל על המשתמש. התוכנה מאפשרת לעצור, להשהות וליצור תהליכים חדשים ומאפרת לשנות את העדיפות של תהליך מסוים.

הפרויקט שלי שואף ליצור תוכנה דמוית Process Explorer ולהציג מידע רב ככל הניתן על כל תהליך ותהליכון שרץ במחשב. כמו כן, הפרויקט שלי שואף ליצור ממשק גרפי מרשים ונוח מאוד עבור המשתמש שיציג את המידע בצורה נוחה לעין. הפרויקט שלי ינגיש את המידע עבור המשתמש הפשוט שאין לו ידע במושגים השונים כגון CPU, socket ועוד וינסה לזהות פרצות אבטחה או התקפות שונות בהתאם לצריכה של תהליכים שונים או בהתאם לנוכחות של תהליכים שונים (למשל, ישנם תהליכים שכאשר הם מופיעים יותר מפעם אחת, הם עלולים להעיד על פרצת אבטחה).

ניתן לייצג את ההבדלים בין המערכות השונות למערכת שלי בטבלה:

|  |  |  |  |
| --- | --- | --- | --- |
| **תבחינים/פרויקט** | **הפרויקט שלי** | **Task Manager** | **Process Explorer** |
| **מידע על תהליכים** | מוצג מידע מורחב על התהליכים- צריכת CPU, סוגי זיכרון מורחבים, תקשורת ועוד | מוצג מידע בסיסי על התהליכים- צריכת CPU, זיכרון private working set, תקשורת ועוד. | מוצג מידע מורחב על התהליכים- צריכת CPU, סוגי זיכרון מורחבים, תקשורת ועוד |
| **מידע על תהליכונים** | מוצג מידע רב על תהליכונים- ה-ID, מצב התהליכון, המעבד האידיאלי עליו רץ התהליכון, צריכת CPU ועוד | לא מוצג מידע מורחב על תהליכונים | מוצג מידע רב על תהליכונים- ה-ID, מצב התהליכון, המעבד האידיאלי עליו רץ התהליכון, צריכת CPU ועוד |
| **מידע על socket ו-pipeline** | מוצג מידע על איזה socket בשימוש ואיזה לא ומציג מידע על pipelines | מוצג מידע על כמות ה-socket שפתוחים | מוצג מידע על כמות ה-socket שפתוחים |
| **אפשרות לשליטה על תהליכים** | מאפשר סיום, השהיה ויצירה של תהליכים | מאפשר סיום תהליכים ויצירת תהליכים | מאפשר סיום, השהיה ויצירה של תהליכים |
| **תצוגה גרפית של התוכנה** | תצורה גרפית מפורטת וברורה שנוחה לעין ונוחה למשתמש | תצוגה גרפית פשוטה ולפעמים לא ברורה | תצורה גרפית מפורטת וברורה שנוחה לעין ונוחה למשתמש |
| **תצוגה גרפית של המידע** | תצורה גרפית כללית של תצרוכת עבור כל תהליך | תצוגה גרפית כללית של תצרוכת | תצוגה גרפית של תצרוכת עבור כל תהליך |
| **זיהוי פרצות אבטחה** | יש | אין | אין |
| **הנגשה למשתמש** | הסבר על מושגים שלא ברורים לאדם הפשוט עם שילוב של תצוגה גרפית מונגשת למשתמש | אין | תצוגה גרפית מונגשת למשתמש |

1. תוצר סופי

3.1 תיאור הפרויקט

המערכת הינה מערכת מסוג system monitor המשמשת לניטור משאבים וביצועים של מערכות מחשב. המערכת עוקבת אחרי משאבים שונים הבהם יש שימוש כמו זיכרון, נתוני רשת ועוד. המערכת מציגה את התהליכים השונים ואת התהליכונים השונים.

למערכת שלי יש שני רכיבים:

* **מחשב-** תוכנה הרצה במחשב של הלקוח ומקבלת מידע על הביצועים השונים של המחשב
* **לקוח-** תוכנה הרצה במחשב הפיזי של הלקוח ומציגה באופן גרפי את הנתונים

כאשר התוכנה תעלה, תוצג גרפיקה עבור המשתמש שהמידע המוצג בה יהיה מידע כללי על התהליכים הרצים במערכת כמו שם התהליך, PID, זיכרון private working set וצריכת CPU. המשתמש יוכל לבחור להתבונן במידע על כל תהליך אותו ירצה או על מידע אחר שלא קשור בתהליכים (למשל, צריכה כללית של המחשב או נתוני socket ו-pipeline).

המשתמש יוכל להתבונן בנתונים השונים ולשלוט בתהליכים השונים המתרחשים במחשב. למשל, לסיים תהליך, להשהות תהליך או ליצור תהליך. המערכת תציג בצורה גרפית ברמה גבוהה את הנתונים השונים על כל תהליך ותהליכון ותאפשר ניתוח סטטיסטי של הנתונים השונים. כל תהליך יופיע במסך הראשי של התוכנה ויהיה צורך בלחיצה כפולה על תהליך על מנת לקבל מידע מפורט יותר.

ממשק המשתמש יהיה נוח ופשוט לשימוש והגרפיקה תהיה ברורה לעין גם עבור המשתמש הפשוט שאין לו ידע קודם בנושא.

המערכת תדע לבצע:

* יצירה, סגירה והשהייה של תהליכים
* צפייה בפרטים של כל תהליך ותהליכון הרצים במחשב המשתמש
* ניתוח סטטיסטי של הנתונים
* זיהוי של מתקפות ופרצות אפשריות בהסתמך על המידע של התהליכים
* תצוגה גרפית ברמה גבוהה שתאפשר הנגשה של המידע ותאפשר נוחות ופשטות בשימוש התוכנה
* תצוגה של sockets ו-pipelines

3.2 אלגוריתמים עיקריים

אלגוריתמים מרכזיים במערכת:

1. קבלת מידע אודות תהליכים במחשב:

האלגוריתם מקבל מידע אודות תהליכים שונים הרצים במחשב ומידע על התהליכונים של כל תהליך על ידי שימוש ב-System.Diagnostics של C#. המידע המתקבל הוא מידע על שם התהליך הרץ, ה-ID שלו (PID), זיכרון private working set, צריכת CPU, נתוני תקשורת ועוד.

3.3 דרישות ואילוצי פתרון

לפרויקט שלי מספר אילוצים:

* המערכת יכולה לרוץ רק על מערכות הפעלה מסוג ווינדוס

לפרויקט מספר דרישות:

* הפרויקט דורש להציג את התצרוכת של כל תהליך על גבי הליבות השונות של המעבד (כלומר על איזה ליבה רץ כל תהליכון).
* הפרויקט דורש לקבל מידע על תהליכים ותהליכונים שונים
* הפרויקט דורש לתמוך בביצועים במהירות מספקת למשתמש
* הפרויקט דורש תצוגה גרפית ברמה גבוהה

3.4 ממשקים למערכות חיצוניות

אין למערכת ממשקים למערכות חיצוניות

3.5 התייחסות לנושא אבטחה

בפרויקט אין היבט אבטחתי.

3.6 ממשק משתמש

3.7 תרחישים עיקריים

1. תצוגה של תהליך מורכב בו ישנם מספר תהליכונים שונים. התהליך יצרוך משאבי תקשורת, זיכרון ומעבד. הפרויקט שלי יצטרך למפות ולקטלג את התצרוכת השונה ולהציג את הנתונים השונים של התהליך.
2. יצירה, סיום והשהיה של תהליך
3. תהליך כתיבת הפרויקט

4.1 תהליך כתיבת הפרויקט

4.2 אתגרים ואופציות שונות למימוש

1. מרכיבי פתרון

5.1 תיחום הפרויקט

* תקשורת- התייחסות וקבלת מידע על sockets ו-pipelines
* אבטחת מידע- אין
* תצוגה- גרפיקה ידידותית למשתמש על ידי שימוש ב-winforms
* מבנה נתונים- שמירת נתונים במערכים, מילונים, משתנים גלובליים ועוד
* מערכות הפעלה- ניטור מידע על אופן ריצה של תהליכים ותהליכונים במערכת הפעלה
* ארכיטקטורת קוד- שימוש בפונקציות רבות
* תיעוד- תיעוד קוד אקטיבי וניהול GIT

5.2 סביבת העבודה (טכנולוגיה)

**שפות התכנות:**

הפרויקט שלי ייכתב כולו בשפת C# עם יישום גרפי של winform.

**סביבות פיתוח:**

Visual Studio עבור שפת C#

5.3 מבט טופולוגי

5.4 מבנה נתונים

5.5 מסד נתונים

5.6 מבט מודולרי

5.7 פירוט מודלים עיקריים

1. תסריטי בדיקה

6.1 דגשים בבדיקה

6.2 תסריטי בדיקה עיקריים

1. רפלקציה

7.1 לוח זמנים מוערך לניהול הפרויקט

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ספטמבר** | **אוקטובר** | **נובמבר** | **דצמבר** | **ינואר** | **פברואר** | **מרץ** | **אפריל** |
| - הגשת הצעת פרויקט ואישורה  - עדכון להצעה כולל POC | - הצגת POC | - הגדרת טיוטת PRD | - קבלת מידע על התהליכונים השונים וסיווגם לפי הליבה עליה רצים | - הוספת sockets ו-pipelines | - יצירת גרפיקה ושליטה על תהליכים, הוספת סטטיסטיקות | - שיפור גרפיקה, הוספת WMI, הוספת זיהוי פרצות  - כתיבת ספר פרויקט | - סיום יצירת גרפיקה ותיקון בעיות שונות  - כתיבת ספר פרויקט |

7.2 אתגרים ותרומה אישית

7.3 תובנות

1. הוראות התקנה ותפעול

8.1 תצורה ודרישות קדם

8.2 התקנה

1. ביבליוגרפיה

במהלך כתיבת הפרויקט הסתמכתי על מספר מקורות מידע:

* <https://stackoverflow.com/>
* <https://learn.microsoft.com/>
* <https://data.cyber.org.il/os/os_book.pdf>

1. נספחים