****

**פרויקט גמר בסייבר**

**מסמך עיצוב**

**גירסה: 1.0**

**שם התלמיד: גיל מנדלבוים**

**מועד הגשה: 24/12/2015**

**הקדמה**

מטרת מסמך האפיון היא לעצב את הפרויקט ולהציג את העיצוב בצורה וויזואלית.

קהל היעד של המסמך הוא אני, מנחי הפרויקט, ובודקי הפרויקט.

המסמך ינחה אותי בדרכי ויעזור לי לבנות את הפרויקט בצורה טובה יותר ומאורגנת יותר- לפי שלבים ובסדר מסוים והגיוני.

**Remote viewer**

המטרה המרכזית של התוכנה היא שליטה במחשבי רשת נוספים, פיקוח וביקורת עליהם וקבלת מידע על המשתמשים בכל אחד ממחשבי הרשת בזמן אמת.

התוכנה מיועדת לחברות גדולות ועסקים אשר מעסיקים עובדים רבים ומשתמשים במחשב (בנק, חברת היי טק וכו).

המוצר יהיה מחולק לשני חלקים עיקריים- השרת (שיפעל מהמחשב המפקח ) והלקוחות (שיהיו כל המחשבים ברשת אשר המנהל רוצה לפקח את התנהלותם).

השרת יהיה אחראי על ניהול התהליכים של כל אחד מהלקוחות, זיהוי פעילות חשודה לפי תהליכים שונית וכמות הזיכרון שתוספים. המנהל יוכל לסגור תהליכים באופן מיידי מרחוק, ויקבל פרופיל משתמש עבור על מחשב ברשת אשר יגדיר את סוג העובד, אופן העבודה שלו, אתרים בהם גולש ושימושו במחשב.

הגדרות:

GUI – ממשק גרפי.

**ארכיטקטורת המערכת:**

**מודולים בצד השרת-**

1.מודול communication= המודול אחראי על התקשורת בין השרת ללקוח (מכיל בתוכו מחלקה לטיפול בהתחברות ומחלקה לטיפול בתקשורת השוטפת עם כל לקוח).

2.מודול security= המודול אחראי על הצפנה ופענוח המידע המוצפן שמגיע לשרת.

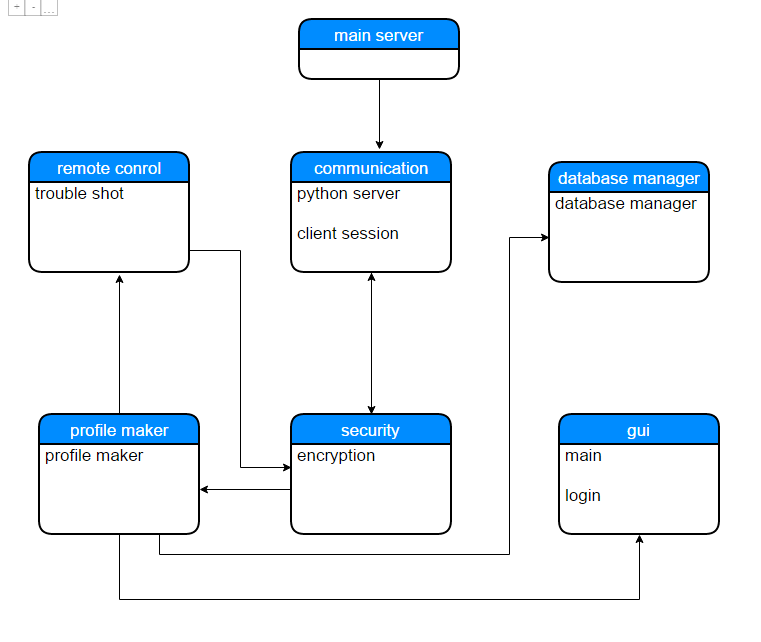
3.מודול profile maker=המודול מקבל את המידע המפוענח (לא מוצפן) ,יוצר פרופיל ללקוח (או מעדכן פרופיל של לקוח קיים) ומחליט האם יש לשמור את המידע שהגיע בdatabase או שהמידע מסוכן ויש לפתור בעיה כלשהי.

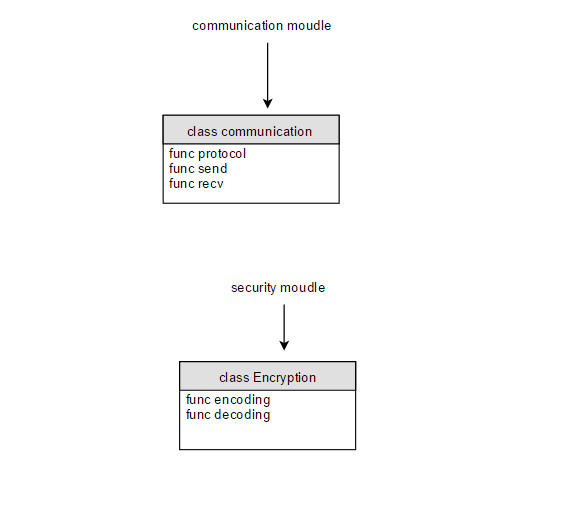
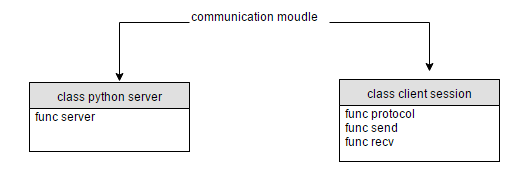
4.מודול remote control= המודול מקבל את המידע הבעייתי לאחר שהשרת יצר פרופיל למשתמש וזיהה מידע בעייתי שעלול להראות על וירוס או שימוש מופרז במחשב- ומחליט כיצד לפעול ואיזו פקודה לשלוח ללקוח בכדי לטפל בבעיה.

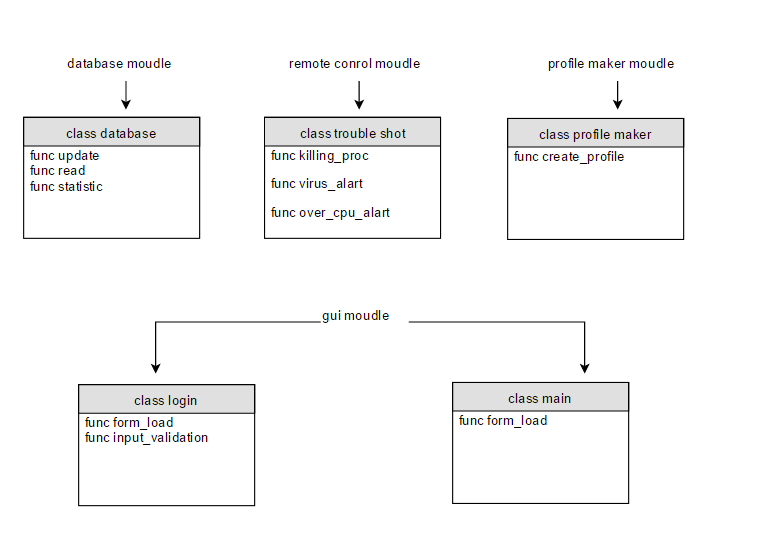
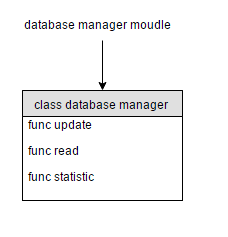
5.מודול manager database= המודול אחראי על הכנסת מידע חדש למסד הנתונים או עדכון מידע קיים- על כל לקוח.

6.מודול gui= המודול אחראי על הצגת הנתונים בממשק ויזואלי.

**Server module diagram**

****

****

****

**מודולים בצד הלקוח-**

1.מודול communication= המודול אחראי על התקשורת בין השרת ללקוח.

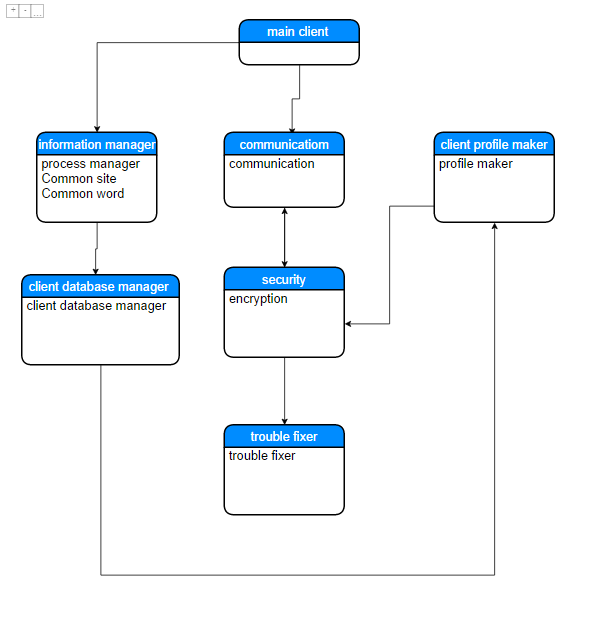
2.מודול security= המודול אחראי על הצפנה של מידע שיוצא מהלקוח ופענוח המידע המוצפן שמגיע מהשרת .

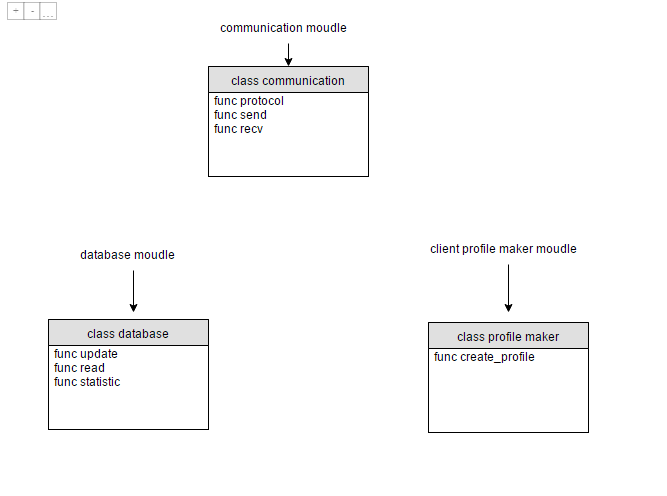
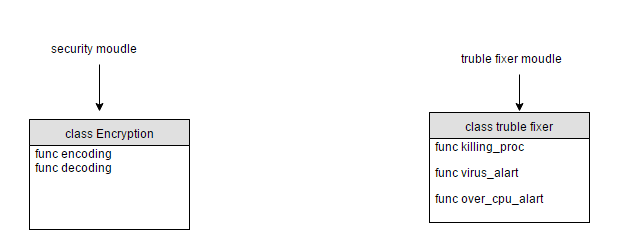
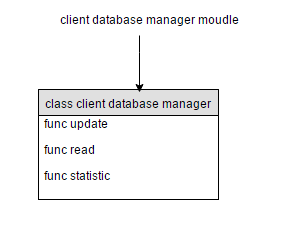
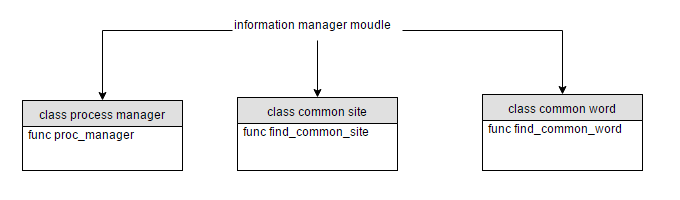
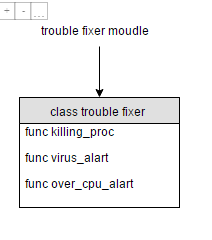
3.מודול information manager= המודול אחראי על איסוף נתונים מהמחשב של הלקוח- מילה שהוקלדה הרבה פעמים, תהליכים נפוצים וכ'ו.

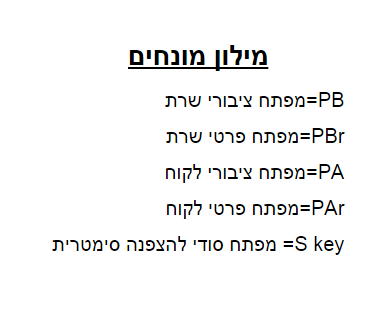
4.מודול trouble fixer= המודול אחראי על פתירת הבעיות שזיהה השרת בצד הלקוח. המודול מכיל בתוכו מחלקה בה יש פעולות לסגירת תהליכים מסוכנים, התראה על שימוש מופרז בזיכרון ועוד.

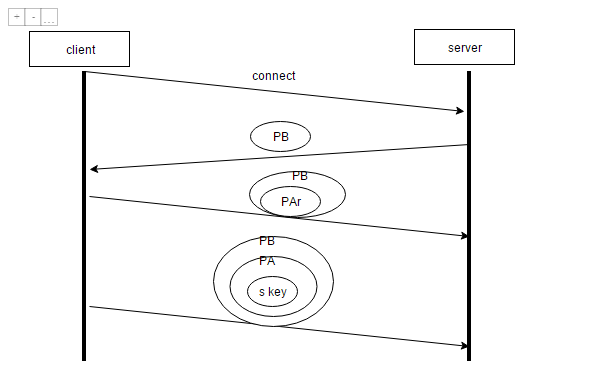
5. מודול client profile maker= יוצר פרופיל זמני למשתמש במחשב אשר מתעדכן ממסד הנתונים ולבסוף שולח את הפרופיל של המשתמש לשרת לשמירה במסד הנתונים של השרת לפי המידע הרלוונטי.

6.מודול client database manager= המודול אחראי על שמירת תהליכים נפוצים, תהליכים רצים, מילים שהמשתמש מרבה לכתוב, פעילות במחשב ושימוש בזיכרון.

**Client diagram**

****

**תרשים החלפת מפתחות לקבלת מפתח סימטרי**



הסבר החלפת המפתחות:

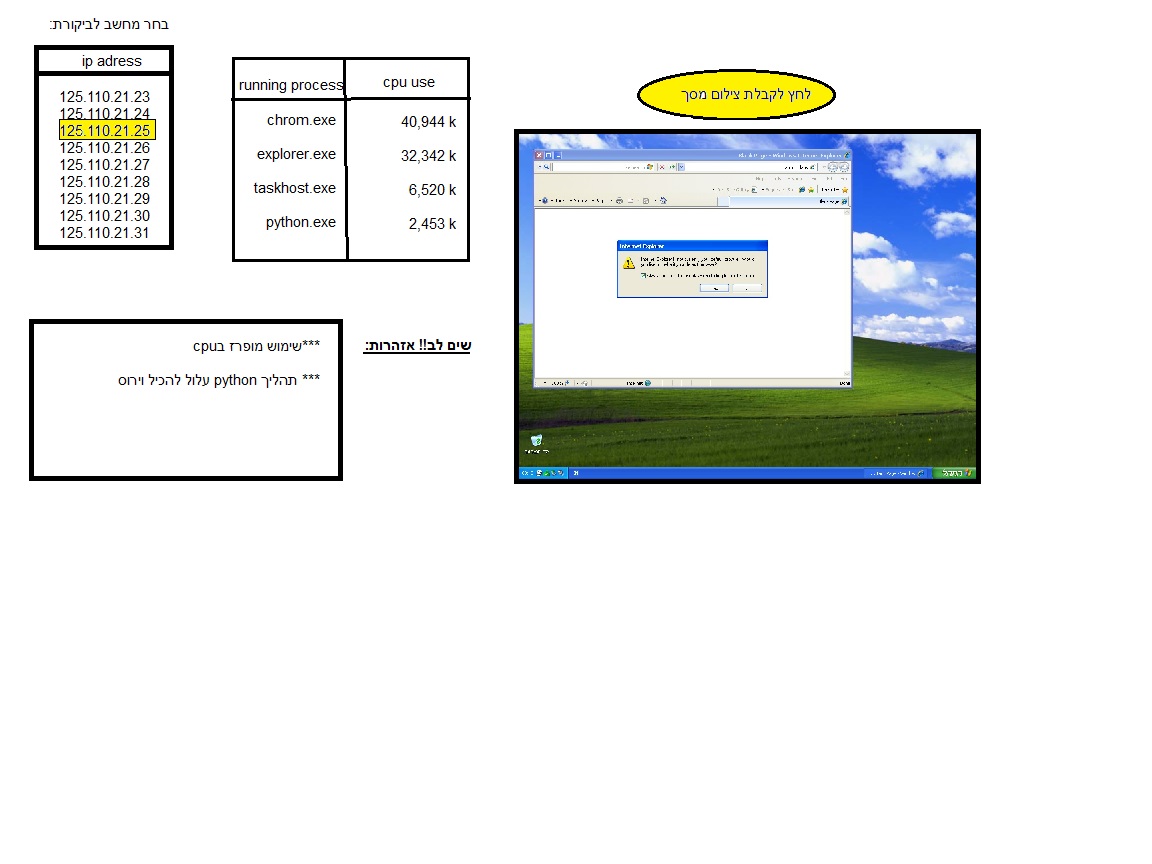
צד הלקוח יוצר בצורה רנדומאלית מפתח להצפנה סימטרית.

הלקוח מתחבר לשרת בעזרת בקשת connect. לאחר מכן השרת שולח ללקוח את המפתח הציבורי של השרת ואז הלקוח שולח לשרת את המפתח הפרטי של הלקוח מוצפן במפתח הציבורי של השרת. ולאחר מכן שולח את מפתח ההצפנה הסימטרית (בו הצדדים ישתמשו להצפנה בהמשך התקשורת), חתום במפתח הציבורי של הלקוח ובמפתח הציבורי של השרת.

לאחר מכן, השרת מקבל את החבילה ויכול לפענח מהו המפתח הסודי להצפנה סימטרית כיוון שבידיו נמצא המפתח הפרטי של השרת ושל הלקוח.

**ממשק משתמש**

****



**תיעוד מחקרים**

במהלך כתיבת הקוד לפרויקט בצד הלקוח- שאמור לדעת לזהות תהליכים מסוכנים (שצורכים הרבה זיכרון או אחוז גבוה של (cpu נתקלתי בקושי. היו תהליכים רבים במחשב שלא הייתה לי גישה אליהם.

בעקבות מחקר שביצעתי במקורות מהאינטרנט ובפורומים של מתכנתים אחרים שנתקלו באותה בעיה הבנתי שבעיה זו נוצרת כיוון שהתהליכים אליהם אני מנסה לגשת הינם תהליכים של המערכת הפנימית ושל הbios ולכן windows לא נותנת גישה אליהם עבור המשתמשים.

בכדי לפתור בעיה זו מצאתי הרשאות שונות בpython בעזרתן ניתן להגיע גם לתהליכים נוספים ולקבל הרשאות לרוב התהליכים הרצים במחשב.

**ניהול עתידי**

|  |  |
| --- | --- |
| **יעדים** | **זמן ביצוע** |
| טיפול הפעלת הclients ברגע הפעלת המחשב | פברואר |
| Data base בצד השרת שמקבל כל כמה דקות עדכונים מהclients המחוברים (כולל קבלת תמונה אם המנהל מבקש לראות תמונת מסך) | פברואר |
| סיום הgui | פברואר- מרץ |
| הגשת דוח ביניים מקיף | 9.3.16 |
| כתיבת תיק פרויקט | מרץ |
| חיבור כל הפרויקט יחד ,בדיקת שגיאות ושיפור ה gui | מרץ |
| הוספת שיפורים ותוספים לפרויקט (לפני המתכונת) | מרץ |
| בחינת מתכונת | 31.3.16 |