

**נושא : מנגנון הגנה תיקיות בחרה**

**שם התלמיד: יונתן חרמץ**

**ת"ז: 207017146**

**בית הספר: תיכון חדש הרצליה**

**שמות המורים: מיכאל צ'רנובילסקי**

**מועד הגשה:14.11.15**

**מבוא**

אחת מהדרישות הכי גדולות בעולם היום היא שמירה על מידע. לכל אחד יש את המידע האישי שלו שעליו הוא היה רוצה להגן מחשיפה לגופים אחרים, בין אם מדובר בחברה או באנשים פרטיים. הצורך הזה נובע מגודל החשיבות של המידע בימינו, ומחשב הוא הדרך הנפוצה ביותר לאכסון מידע. לכן, ישנם אנשים רבים שמנסים להגיע למידע פרטי אשר לא שייך להם- בין אם דרך הרשת באמצעות מחשב אחר ובין אם באופן פיזי שבו אדם לוקח מידע ממחשב שאינו שלו.

הרעיון שלי לפיתוח הפרויקט נובע בעצם מאותו צורך בסיסי להגן על מידע רגיש. במסגרת לימודי רשתות ומערכות מחשבים הבנתי באיזו קלות יכולים אנשים לדלות מידע מהמחשב שלך ללא ידיעתך. הגעתי למסקנה שיש צורך גדול מאוד לשמור על המידע שלך, בצורה פשוטה וקלה לתפקוד.

התוכנה אמורה למנוע גישה פיזית של אנשים זרים לקבצים ותיקיות חשובות על ידי בקשת שם משתמש וסיסמה בעת ניסיון כניסה לתיקייה חשובה. ברגע שאותו זר מכניס פרטים לא נכונים או מתמהמה- הודעה נשלחת לשרת והתיקייה עוברת הצפנה באופן אוטומטי. כמו כן, אותו תהליך עובר בעת ניסיון הכניסה בכל שאר הלקוחות- בכל מחשב נוסף אשר מחובר לשרת ונמצאת בו אותה תיקייה רגישה, התיקייה בו עוברת גם היא הצפנה. בנוסף לכך המחשב לא ימשיך לתפקד עד להודעה מהשרת בכדי למנוע ניסיון פיצוח של ההצפנה. הצפנת התיקייה תבוטל רק לאחר הודעה מהשרת, לאחר שהאיום הפסיק.

**תיאור המוצר**

המטרה המרכזית של המוצר היא למנוע מגורם זר לקבל גישה לתיקיות רגישות הנמצאות במחשב. השרת שמחובר למספר לקוחות מחובר גם לבסיס נתונים אשר נמצאים בו פרטי שם משתמש וסיסמה אשר שיכים לכל אחד מהלקוחות. בעת ניסיון כניסה לתיקייה רגישה, המערכת תבקש מהמשתמש לאמת את נתוני הגישה שלו. במקרה והנתונים שהוזנו לא נכונים או המשתמש התמהמה יתר על המידה בעת הכנסת הנתונים- התיקייה הרגישה תוצפן והמחשב יפסיק להגיב למשתמש.

הצפנת התיקיות תתבצע על ידי מפתח אשר יתקבל מהשרת, ופיצוח התיקייה והמשך פעולת המחשב יתבצעו רק לאחר אישור מהשרת. אותה פעולה של הצפנת התיקייה ואי תגובת המחשב תתבע גם בכל שאר הלקוחות של השרת אשר ברשותם אותה תיקייה רגישה או נמצאים ברשת משותפת עם המחשב שבו התרחש ניסיון הפריצה- בכדי למנוע פריצה של המחשב דרך מחשב אחר הנמצא באותה רשת.

Data Base

Decryption key

Server

Client

Client

קיימות שני יישומים :

1. **יישום שרת מכיל :**

* **מודול**

1. **יישום לקוח**

**אילוצים ודרישות**

הבעיות שהמערכת צריכה לדעת להתמודד איתן הן:

1. ניסיון חדירה לתקשורת בין השרת הלקוח על מנת להשיג את מפתח ההצפנה.
2. מי שמנסה להגיע לתיקייה רגישה עלול לפצח את הצפנת התיקייה.
3. ישנה אפשרות לנסות לקבל גישה לתיקייה הרגישה דרך מחשב אחר הנמצא באותה הרשת.

היא נותנת להן מענה בכך ש:

1. הצפנה נוספת של התקשורת בין השרת ללקוח.
2. הודעת הזהרה נשלחת לשרת בעת ניסיון פריצה והמחשב נחסם לשימוש עד לאישור מהשרת.
3. לאחר ניסיון פריצה, על המחשבים הנמצאים באותה הרשת מקבלים הודעת הזהרה ונחסמים גם הם לשימוש.

**תיחום הפרויקט**

הפרויקט עוסק בתקשורת מחשבים, בעבודה עם מערכת ההפעלה Windows ובאבטחת מידע.

המודולים שבהם המערכת משתמשת הם: שרת מרכזי ולקוחות (המחשבי הרשת) שמחוברים באמצעות socket, הצפנת המידע העובר בתקשורת, בסיס נתונים המכיל פרטי שם משתמש וסיסמה של הלקוחות, מודול שמאפשר לקבל הצפנת תיקיות רגישות בעת הצורך, מודול שמאפשר חסימה של המחשב ומניעת שימוש בו ולבסוף ה- GUIבצד השרת ובצד הלקוח.

**סביבת העבודה**

הפרויקט ייכתב ב- Python וב- C#. עיקר הקוד של הפרויקט (כל החלק האחראי על התקשורת בין המחשבים, על השליטה מרחוק, על הצפנת המידע) ייכתב ב- Python בשל פשטות ונוחות השפה, וה- GUI ייכתב ב- C# כי הרבה יותר נוח לכתוב GUI ב- C# מאשר ב- Python.

סביבות העבודה והכלים הנדרשים לפיתוח הם: PyCharm לכתיבת הקוד ב- Python ו- Microsoft Visual Studio 2010 על מנת לכתוב את ה- GUI ב- C# באמצעות גרירת פקדים מה- toolbox.

סביבות העבודה והכלים הנדרשים לבדיקות הם: Command Prompt (cmd) בשביל הרצת הקוד שנכתב ב- Python (שרת ולקוח) ובדיקה שזה עובד וה- debugger המובנה ב- Microsoft Visual Studio 2010 לבדיקת תקינות הקוד ב- C#, תקינות החיבור בין ה- Python וה- C#, ובדיקת פעולתה התקינה של המערכת באמצעות ה- GUI.

**ניהול פרויקט עתידי**

|  |  |
| --- | --- |
| **יעדים** | **זמן ביצוע** |
| מחקר לגבי הרכיבים הנדרשים בשביל המערכת (קבלת מידע לגבי הצפנת קבצים ,הצפנת תקשורת,חסימת מחשב ועוד) | דצמבר |
| כתיבת שרת ולקוח ב- Python כך שהשרת מותאם לטפל במספר לקוחות בו-זמנית. הצפנת המידע הנשלח. | דצמבר |
| כתיבת בסיס נתונים המכיל את כל פרטי המשתמשים | ינואר |
| כתיבת מודול המצפין תיקיות וקבצים חשובים. | ינואר |
| כתיבת מודול המונע שימוש נוסף המחשב לאחר ניסיון פריצה. | ינואר או פברואר |
| כתיבת דו"ח ביניים. | סוף ינואר (הגשה ב-1 בפברואר) |
| חיבור כל המודולים ביחד, בדיקות ותיקון שגיאות. | פברואר |
| כתיבת ה- GUI וחיבורו לחלק שנכתב ב- Python. | פברואר + מרץ |
| עוד בדיקות ותיקון שגיאות. | מרץ + אפריל |
| כתיבת תיק הפרויקט. | אפריל |
| תוספות ושיפור הפרויקט. | אפריל + מאי |