**SafeStorageLock**

מסמך אפיון

1.3.5

5.1.16

רועי אופק ומור שמש

**הסטוריית גרסאות המסמך**

|  |  |  |  |
| --- | --- | --- | --- |
| **תאריך** | **עורך/ת** | **תיאור / תקציר השינויים** | **הערות נוספות** |
| **2.11.15** | **מור ורועי** | **התחלה** | **שיחת סקייפ בין שנינו** |
| **10.11.15** | **מור ורועי** | **סיבוב שני - השלמת החסר ומיקוד** | **שיחת סקייפ בין שנינו** |
| **25.11.15** | **מור ורועי** | **ניקיון המסמך** | **מחיקת הערות** |
| **25.11.15** | **מור ורועי** | **חידוד והרחבה, הוספת התמונות** |  |
| **1.12.15** | **מור ורועי** | **עריכה, הסרת התמונות** |  |
| **16.12.15** | **מור ורועי** | **הורדת האופציה לחיבור Wi-Fi, הוספת תרשימים** | **שיחת סקייפ בין שנינו** |
| **23.12.15** | **מור ורועי** | **תיקונים והערות** |  |
| **27.12.15** | **מור ורועי** | **חזרה לשימוש בתקשורת Wi-Fi, ויתור על תקשורת Bluetooth מסיבוכים** | **שיחת סקייפ כרגיל...** |
| **5.1.16** | **מור** | **חזרה לBluetooth** |  |

תיאור כללי:

מערכת, SafeStorageLock, הינה מערכת לאבטחת קבצים במחשב באמצעות הצפנתם . נעילת ופתיחת הקבצים נעשות ממכשיר טלפון אשר עליו להמצא בסמיכות למחשב ולהיות מקושר אליו באמצעות ממשק Bluetooth אחרת לא יהיה ניתן לפתוח את הקבצים. על הטלפון אפליקציה המאתרת מחשבים עליהם התוכנה מותקנת ומוכנה. הטלפון יציג רשימת מכשירים אפשריים לפעולה וידרוש סיסמא בהתאם לכל אחד מהם. הסיסמא תישמר באחריות המשתמש. ה"נעילה" תתבצע על-ידי הצפנת המידע שמרכיב את הקבצים - הצפנה סימטרית. לכן המערכת מכילה שני חלקים: טלפון Android ומחשב Windows.

**1.2 הגדרות**

SafeStorageLock

טלפון - הטלפון המתקשר עם המחשב, על הטלפון להיות "חכם" (יענו אינטיליגנט) ולהריץ מערכת Android.

מחשב - המחשב הוא המרכיב המאחסן את הקבצים. על המחשב צריכה לפעול מערכת Windows מגירסה 7 ומעלה.

מנגנון הנעילה - התוכנה במחשב שאחראית על הצפנת הקבצים.

הצפנה: מנגנון הסתרת תוכן הקבצים. ההצפנה תמומש באלגוריתם AES256.

הקוד כתוב בשפה:

מחשב - C#

בטלפון *-* Java

**2. תיאור כללי**

**2.1 פונקציונליות**

1. נעילת קבצים על המחשב בתיקייה ייעודית, המשתמש יבקש פתיחה/נעילה במחשב, תועבר בקשת סיסמא לטלפון. לכל משתמש תיקייה משלו, שאינה נמצאת באף תקייה מאובטחת של משתמש אחר.
2. פתיחת הקבצים הנעולים, ניתן להיעשות אך ורק מהטלפון.
3. מאפשר צפייה במעקב (log) אחרי הנעילות והפתיחות, כולל כישלונות, מהמחשב או הטלפון.
4. כל התקשורת נעישת בצורה מאובטחת ומוצפנת בהתאם לפרוטוקול שנקבע על ידינו.
5. פעולה במוד של Fail Safe דהינו בכל תרחיש שלא צויין לרבות אובדן תקשורת בין הטלפון למחשב וכיוצ”ב הקבצים יעברו למצב מוצפן או ישארו מוצפנים.

**2.2 מאפייני משתמשים**

קהל היעד הוא כל מי שמעוניין לשמור על הקבצים שלו שיהיו מוגניםמגניבה/העתקה/שיבוש, בהינתן שיש להם טלפון Androidתואם ומחשבWindows.

**2.3 אילוצים עיקריים**

כיצד מתחברים, מתנהלים בין האפליקציה והתוכנה - "היכרות" בין מחשב וטלפון של משתמש מסויים תיאלץ להתבצע פעם אחת בדיוק, ואחריה יהיה צורך רק בהתחברות בתחילת כל פעילות עם תיקיית הקבצים המאובטחת.

**2.4 הנחות ותלויות**

1. התוכנה במחשב רצה על Windows, מחשב שיש לו חיבור Bluetooth
2. האפליקציה בטלפון מיועדת למכשירי אנדרואיד. המכשיר עם חיבור Bluetooth.
3. מתקיים חיבור בין המכשיר הסלולרי למחשב, כאשר שניהם במרחק קצר

זה מזה ומקיימים תקשורת בינהם.

**3. דרישות מפורטות**

כל המערכת מבוססת על אבטחת מידע - התקשורת בין הרכיבים מוצפנת, הקבצים המוגנים חסרי משמעות לאחר נעילה למען שמירה עליהם ואסור למערכת בשום אופן לפגוע בקבצים בעת תקלות בזמן העבודה איתם.

אימות הסיסמא ייעשה ע"י הצפנת קובץ ייעודי במחשב שאינו נגיש למשתמשים וניסיון הצפנה/פענוח שלו.

**3.1 דרישות פונקציונליות**

סנכרון ראשוני עם המחשב - (מסתמך על דרישה מס' 5)

פעולה המתבצעת פעם אחת ע"י משתמש המאפשרת עבודה עם המערכת, מסנכרנת בין המחשב לטלפון.

לאחר שהמשתמש הוריד את האפליקציה לטלפון והתוכנה למחשב, המשתמש יזין שם משתמש בשני הקצוות. שני המכשירים צריכים להיות מחוברים בBluetooth. כשיימצא את המחשב המבוקש, שייבחר ע"י המשתמש, יתבצע סנכרון ראשוני - המחשב יירשום את פרטי הטלפון והטלפון ירשום את פרטי המחשב כלומר, בשני הקצוות יתקיימו יומנים נפרדים של פרטי המכשירים.

לאחר ה"הכרות", המשתמש יתבקש לפתוח תיקייה בה ירצה לשמור את קבציו. תחת תקייה זו יישמרו כל הקבצים שהתוכנה תגן עליהם. המשתמש ייתבקש להזין סיסמא בה יישתמש על מנת לנעול ולפתוח את קבציו.

התחברות -

פעולה הנדרשת להתבצע בכל פעם שרוצים לנעול או לפתוח קבצים במחשב.

המשתמש מחפש בטלפון מחשב זמין (מחשב שמותקנת עליו המערכת ושיציג את שם המשתמש בו) בBluetooth. לאחר מציאת המחשב, שתבוצע לפי שם משתמש, יוסדר החיבור בין שני הקצוות ויישאר פתוח ויחכה שהמשתמש יבקש לנעול או לפתוח קבצים במחשב.

**קובץ נעול** הינו קובץ שהוצפן כל תוכנו בצורה שלא מאפשרת שימוש במידע שלו. מבחינת אדם מבחוץ שמסתכל על הקובץ הוא יראה אוסף חסר משמעות של תווים.

נעילת קבצים - (מסתמך על סעיפים 3.1.1-4)

לאחר שהמשתמש ביצע חיבור, תנתן לו האופציה לבחור תקיות וקבצים אותם הוא יכול לנעול. לאחר שסימן אילו קבצים הוא רוצה לנעול(ניתן לסמן תקייה, וכל מה שבתוכה יוצפן), תישלח הודעת בקשת נעילה לטלפון. בטלפון תוצג הודעה שהתבקשה נעילת קבצים במחשב. המשתמש יוכל לבחור בין שתי אופציות - סירוב או אישור. במקרה של סירוב לא יידרש דבר נוסף. במקרה של אישור תידרש סיסמא, וכשתאומת במחשב יינעלו הקבצים עם הצגת הודעה מתאימה במחשב, ורישום ביומן שבמחשב.

פתיחת קבצים - (מסתמך על סעיפים 3.1.1-4)

לאחר שהמשתמש ביצע חיבור, תנתן לו האופציה לבחור תקיות וקבצים אותם הוא יכול לפתוח. לאחר שסימן אילו קבצים הוא רוצה לפתוח (ניתן לסמן תקייה, וכל מה שבתוכה ייפתח), תישלח הודעת בקשת פתיחה לטלפון. בטלפון תוצג הודעה שהתבקשה פתיחת קבצים במחשב. המשתמש יוכל לבחור בין שתי אופציות - סירוב או אישור. במקרה של סירוב לא יידרש דבר נוסף. במקרה של אישור תידרש סיסמא, וכשתאומת במחשב ייפתחו הקבצים עם הצגת הודעה מתאימה במחשב, ורישום ביומן.

אופציונלי - בדיקת תקינות תקשורת כתנאי לעבודה עם הקבצים הפתוחים. (keep alive): המשתמש יוכל לאפשר פיצ'ר שידאג שברגע שהשתבשה התקשורת בין המחשב והטלפון המשתמש יותרע על כך.

דרישה: ייתקיים בסיס נתונים טקסטואלי המחזיק את יומן הפעולות שבוצעו במחשב ובטלפון, בכל מכשיר יומן נפרד משלו.

ביצוע:

צפייה ביומן -

המשתמש ייכנס דרך התוכנה ליומן הפעולות של המחשב או באפליקציה ליומן הפעולות שבטלפון.

הנחיות ודרישות לכל הפיצ'רים במערכת:

**3.1.1** הצפנה - כל הקובץ מוצפן. אסור שהקובץ יינזק בעת ניסיון פתיחה/נעילה כושל או כל מקרה קצה אחר.

**3.1.2** כאשר המשתמש רוצה להתחיל בשימוש בקבצים - נעילה או פתיחה - לחיצת כפתור באפליקציה תורה לטלפון לחפש מחשבים תואמים בBluetooth ולהציג אותם למשתמש.

**3.1.3** במחשב כל תיקייה עליה אנחנו אחראיים - תשויך למשתמש מסויים שלו מפתח ייחודי. פתיחת הקבצים תתבצע לפי קבצים בודדים או תיקיות.

**3.1.4** הסיסמא אינה שמורה באף צד של המנגנון (הטלפון או המחשב). במקום זאת, נסיון פתיחת קובץ ייעודי יאשר את אמיתות הסיסמא.

**3.1.5** לכל משתמש (צד טלפון וצד מחשב) יהיה מספר זיהוי ייחודי, על מנת לאמת תקשורת. המספר הזה יישמר גם על המחשב וגם על הטלפון. לכל משתמש סיסמא ייחודית לו שנקבעה בעת הסנכרון.

**3.2 דרישות של ממשקים חיצוניים**

**3.2.1 ממשקי משתמש**

ממשק משתמש באנגלית, ממשק ברור ואינטואיטיבי.

**3.2.2 ממשקי תוכנה**

טלפון: ממשק Android,

מחשב: עבודה עם ממשק Windows, סביבת ריצה CLR .NET runtime framework

**3.2.3 ממשקי תקשורת**

Bluetooth

**3.3 דרישות לא פונקציונליות**

אם נרצה להתאים את התוכנה לשימוש במסגרות בעלות רגישות גבוהה לרמת האבטחה, מומלץ לעקוב אחרי הקווים המנחים בהפניות [1] ו[2] בעקרונות "CIA".

**3.3.1 דרישות אמינות (reliability)**

אמינות - לפני כל תהליך הצפנה או פתיחה יהיו גיבויים כך שלא יהיה מצב בו הקובץ נהרס בעת השימוש במערכת שלנו.

**3.3.2 דרישות זמינות (Availability)**

זמינות - ממשק נוח למשתמש, לא דורש ידע בהצפנה או תכנות כלל.

**3.3.3 דרישות אבטחה (security)**

אבטחה - כל התקשורת בין הטלפון למחשב מוצפנת, הסיסמא אינה שמורה על המחשב או הטלפון למען אבטחה מירבית. (SSL)

**מניעת נסיון פריצה באמצעות Brute force -**

השהייה, רישום בlog, התרעה

**3.3.4 דרישות תחזוקה (maintainability)**

תחזוקה - קיום יומן פעולות טקסטואלי מלא של כל התהליכים שהתרחשו במערכת.

**3.4 דרישות בסיס נתונים**

בסיס נתונים טקסטואלי ששומר את יומן הפעולות של המערכת

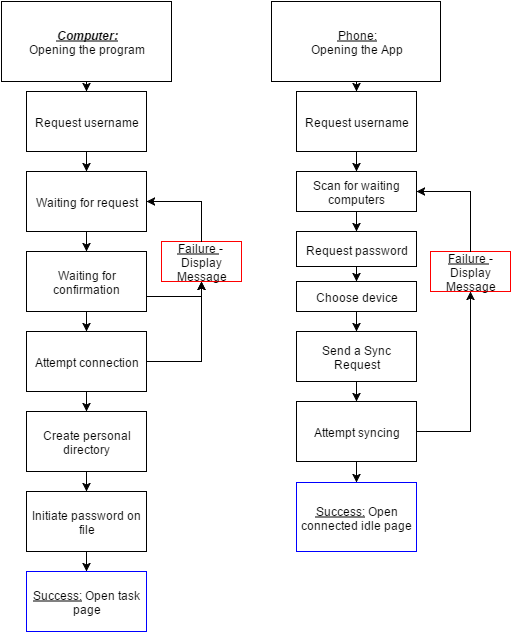
**3.5 דרישות נוספות**

אחריות של המשתמש לשמור את סיסמתו. הסיסמא תאומת מול קובץ ייעודי.

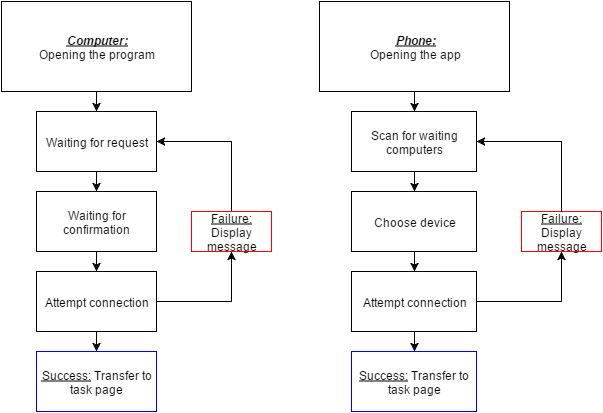
**4. כלי ניתוח**

**4.1 state-Transition Diagrams (STD)תמונות**

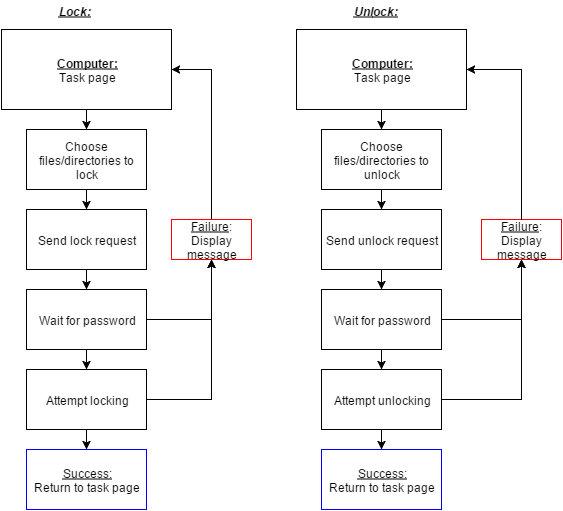
תהליך סנכרון ורישום ראשוני - מחשב + טלפון:



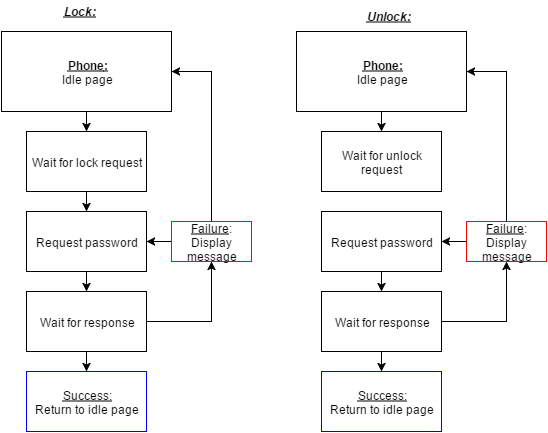
תהליך חיבור ראשוני בין מחשב לטלפון לפני תחילת העבודה - מחשב + טלופן:



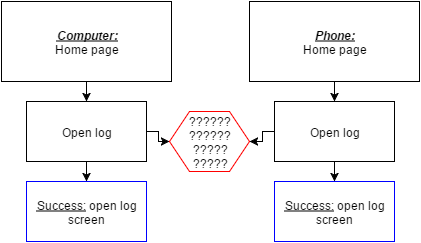
תהליכי השימוש במערכת 1: נעילה ופתיחה - מחשב:



תהליכי השימוש במערכת 1: נעילה ופתיחה - טלפון:



תהליך השימוש במערכת 2: צפייה ביומן - מחשב + טלפון:



**5. הפניות**

*חלק זה צריך לכלול את כל המקומות אליהם אתם מפנים לאורך המסמך (מסמכים אחרים שכתבתם או מסמכים באינטרנט) . כל הפניה צריכה לכלול כותרת,מקור,ואת הלינק עצמו.*

*לדוגמא:*

1. <http://www.techrepublic.com/blog/it-security/the-cia-triad/>
2. <http://ishandbook.bsewall.com/risk/Methodology/CIA.html> *עקרונות ודרישות מערכות אבטחת קבצים סטרנרטיות.*