בס"ד

ROUTE TRACING

דו"ח מסכם בפרויקט סיום בקורס מערכות להרצת קוד בסביבה בטוחה
שנת תשפ"א סמסטר א
המרכז האקדמי לב – המחלקה למדעי המחשב

מנחה: מר ברק עינב
מגישות: אלינוי גדעוני 209350958
תמרה צבאן 318252756

Table of content

Presentation in Code Execution Systems in a Trusted Execute Environment Course

Final Report

Name of Project

Route Tracing

Introduction

כחלק מהלוחמה במגפת הקורונה, הוחלט בממשלת ישראל כי על מנת לצמצם את מספר הנדבקים באופן משמעותי יש לנקט באמצעים משמעותיים שיכללו התחקות ומעקב אחר חולי הקורונה ב14 יום שקדמו להידבקותם בנגיף.

לצורך כך, הוחלט בממשלת ישראל, כי הטלפונים הניידים של חולי הקורונה יאוכנו וכך לשב"כ יהיה את כל המידע על מקום הימצאותם של החולים ב14 יום האחרונים, את הנתונים הללו הוחלט לפרסם באמצעי התקשורת וברשתות החברתיות ובכך ליידע את הציבור הרחב על מקומות, שעות ותאריכים בהם שהו חולי הקורונה ובכך לעזור להם להתגונן מפני המגפה.

The Problem

החלטה זו שהתקבלה בממשלת ישראל הביאה אחריה הדים רבים וסערה תקשורתית רחבה. אנשים הביעו כעס רב וחוסר אמון במערכת השלטון והרגישו כי פרטיותם וחיסיון פרטיהם נפגע עד מאד.

"הזכות לפרטיות, הזכות הנפגעת העיקרית בהצעה, זכתה במדינת ישראל למעמד של זכות חוקתית, מכוח קביעתה במסגרת סעיף 7 לחוק יסוד: כבוד האדם וחירותו. פיסקת ההגבלה בחוק היסוד דורשת, כידוע, קיומם של מדדים ברורים אשר יאפשרו פגיעה בזכות היסוד, כמו תכלית ראויה, מידתיות, סבירות וצמידות מטרה. לטעמנו, אלה לא מתקיימים בתקנות." – זוהי רק אחת מני אלף התבטאויות שנאמרו כנגד האיכון על הטלפונים הסלולריים.

ובצדק, עצם הידיעה כי בוצע איכון על המכשיר הסלולרי על כל תכולתו גורמת לכעס רב בקרב הציבור ופוגעת בפרטיות.

The Solution

הפתרונות שיש כיום למעקב ולבקרה אחרי אנשים שחלו בקורונה או נחשפו לחולה מאומת מעוררים מחלוקת, ובראשם טכנולוגיית האיכון הסלולרי של השב"כ. זאת, עקב הפגיעה בפרטיות.

חשבנו כי במקום שהשב"כ יבצע איכון על הטלפון הסלולארי של האזרח, תהיה אפשרות להוריד אפליקציה ייעודית שמטרתה היא איסוף המידע הרלוונטי בלבד עבור התחקות אחר חולה קורונה. כלומר הפרטים היחידים שישמרו יהיו הקומות התאריכים והשעות בהם ביקר החולה המאומת ב14 יום שקדמו לאימות כי נדבק בנגיף.

פרטים אלו עדיין מהווים מידע רגיש מאד, אף אדם לא רוצה שהציבור הרחב יקבל מידע על הימצאותו והמקומות בהם בילה. עם זאת עומדת לנגד עיננו מטרה חשובה עד מאד והיא לוחמה בנגיף שתביא למיגור המגיפה כאשר חלק מהצעדים הם התחקות אחר חולים מאומתים.

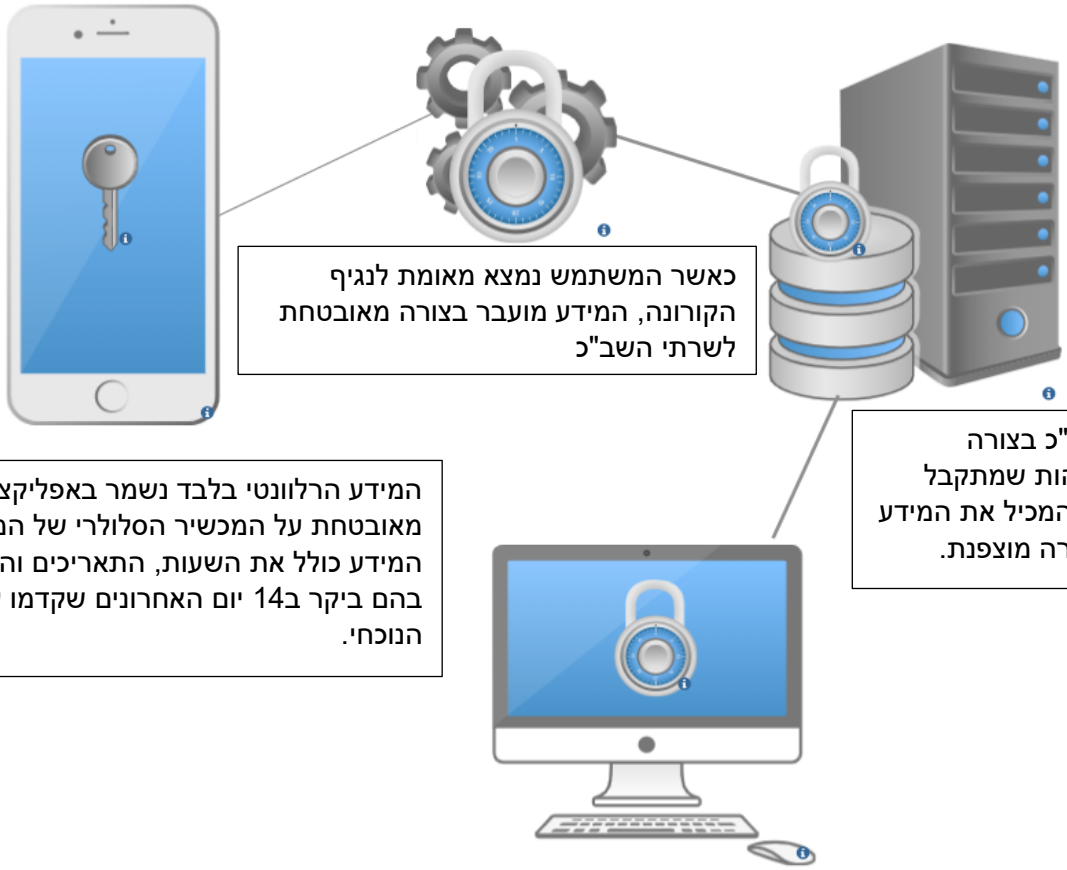
אותו מידע שישמר באפליקציה, יועבר לשרתי השב"כ בצורה מאובטחת וישמר באופן מוצפן. בנוסף יש לקשר בין מספר הזהות של החולה המאומת לבין רשימת המקומות בהם ביקר. הקשר הזה הוא סודי ביותר ולכן נרצה להבטיח כי מספר הזהות של החולה המאומת שמשמש מזהה ייחודי יתקשר אך ורק למידע הספציפי של אותו חולה מאומת. כך שגם אם יש איזשהיא פרצה למערכת, לא תהיה חשיפה של המידע כולו אלא רק באופן נקודתי.

אנחנו חושבות כי הייחודיות בפרויקט ומעלותיו על השיטות הקיימות כיום הן:

1. לא מתבצע איכון מקיף על כל תכולת הטלפון של האזרח, אלא המידע המועבר הוא ספציפי ביותר, בדיוק מה שצריך- את המיקומים, השעות והתאריכים בהם ביקר החולה המאומת.
2. נוסף לכך, אותו איכון חלקי אינו מתבצע על מכשירי הסלולאר של כלל האזרחים אלא רק על אזרחים שאומתו חיוביים לנגיף הקורונה.
3. הנתונים שמועברים לשב"כ נשמרים בצורה מוצפנת, כך שלאדם מהשורה – גם אם עובד בשב"כ, עדיין אין גישה לנתונים.
4. כאשר יהיה צורך בעדכון אנשים ששהו בקרבת אותו אדם שאומת לקורונה, הם יקבלו הודעת sms ספציפית ולא פרסום נרחב ברשתות החברתיות ובאמצעי התקשורת.
5. אין גישה ישירה לנתונים, כלומר אין אפשרות לגשת לנתונים של כלל החולים המאומתים בצורה ישירה. הגישה תהיה אך ורק באמצעות שאילתה של "האם אדם עם מספר תעודת זהות x, היה במקום y בתאריך z.
6. הכניסה לאותה מערכת שאילתה תהיה מותרת אך ורק לעובדי שב"כ מורשים באמצעות שם משתמש וסיסמא.

ע"י נקיטה באמצעים אלו ופרסומם לציבור, אנו חושבות כי אמון הציבור יגדל וכי החשש לפגיעה בפרטיות יקטן. בעזרת אמצעים אלו נוכל להגן על פרטיות הציבור שזו זכות בסיסית לחלוטין של כל אדם.

Design and Architecture



כאשר המשתמש נמצא מאומת לנגיף הקורונה, המידע מועבר בצורה מאובטחת לשרתי השב"כ

המידע נשמר בשרתי השב"כ בצורה מוצפנת. עבור כל מספר זהות שמתקבל במערכת נוצר קובץ ייעודי המכיל את המידע שהועבר מהאפליקציה בצורה מוצפנת.

המידע הרלוונטי בלבד נשמר באפליקציה מאובטחת על המכשיר הסלולרי של המשתמש. המידע כולל את השעות, התאריכים והמקומות בהם ביקר ב14 יום האחרונים שקדמו לתאריך הנוכחי.

הגישה למידע השמור בשב"כ תתבצע רק למשתמשים מורשים כך שהכניסה למערכת תתבצע באמצעות הזנת שם משתמש וסיסמא. בנוסף לאחר הכניסה למערכת, לא תהיה גישה מלאה לכל הקבצים השמורים בשרת, אלא תהיה אפשרות לבצע שאילתא בה המשתמש המורשה יתבקש להכניס מספר זהות ומיקום שעה ותאריך והוא יוכל לקבל תשובה האם אותו אדם בעל מספר זהות מסוים נכח באותו מקום בזמן ספציפי.

Threat Model

למעשה, הערך החשוב לנו ביותר היא פרטיות האזרח

הזכות לפרטיות היא זכותו של אדם למרחב פרטי פיזי או וירטואלי הנתון לשליטתו, מתוך ההכרה כי ישנם תחומים בחיי אדם שאינם אמורים להיות ברשות הרבים ללא הסכמתו המפורשת. הזכות לפרטיות היא חלק מזכויות האדם הטבעיות, להן זכאי כל אדם באשר הוא, משום שכל אדם זקוק לפרטיות על מנת לפתח ולממש את האוטונומיה שלו כפרט. הפרטיות מאפשרת לאדם לחיות את חייו ולשלוט על מידת החשיפה של חייו בהתאם לרצונו, ללא חשיפה, התערבות או חדירה לחייו.

הזכות לפרטיות הינה בזכות יסוד, המוגנת באמנות ובהסכמים בין-לאומיים , כמו גם בחקיקה בישראל ובעולם. מרבית החוקים בעולם מגבילים את הפרטיות כאשר היא מתנגשת בזכויות ובאינטרסים ציבוריים אחרים, כמו למשל :חופש הביטוי ,חופש המידע ,זכות הציבור לדעת ,ביטחון ציבורי ועוד

המשפטן האמריקני דניאל סולוב מציע טקסונומיה של קטגוריות של מצבי פגיעה בפרטיות במטרה להסיט את הדיון התאורטי והמשפטי בהגדרת מושג ה-"פרטיות" אל עבר ציון הפעילויות שמציבות איום על הפרטיות:

1. איסוף מידע: (1) מעקב, (2) חקירה
2. עיבוד מידע: (3) צבירת מידע, (4) זיהוי על בסיס מידע , (5)אבטחת מידע (6) ,שימושים אחרים במידע, (7) היעדר שקיפות כלפי מושא המידע
3. הפצת מידע: (8) הפרת אמון, (9) גילוי מידע, (10), חשיפה, (11) הגברת תפוצה של מידע, (12) סחיטה, (13) נטילת זהות, (14) עיוות מידע
4. חדירה: (15) פלישה, (16) התערבות בהחלטות

ניתן לראות כי הפעולות הנ"ל מהוות איום על הפרטיות, הערך עליו אנו רוצים לשמור.

Mode of work and Challenges

לינוי ואני עבדנו יחד בשיתוף פעולה מלא. אנחנו רגילות לעבוד יחד בקורסים נוספים כך שהולך לנו טוב ביחד.

עבדנו על הפרויקט בזום באופן הבא:

לינוי עבדה על המצגת, ואני עבדתי על הדוח המסכם. כמובן שהיינו בקשר רציף והתייעצנו אחת עם השנייה וחידדנו דברים שלא היו לנו מובנים.

את העבודה על הפרויקט ברמת הקוד עשינו ביחד ממש, קודם כל תכננו את הארכיטקטורה הרצויה בפרויקט ווידאנו שבכל שלב אנו מיישמות את הנלמד במהלך ההרצאות. לאחר מכן כתבנו את המחלקות והפונקציות.

מובן שנתקלנו בקשיים במהלך הפרויקט, דוגמא לכך, זה עצם התכנות בשתי סביבות עבודה שונות, בשתי שפות שונות. אמנם יצא לנו לכתוב תוכניות בין שרת ללקוח אך באותה סביבת עבודה.

נוסף לכך, לקח לנו קצת זמן להבין איך התקשורת בין ה host ל applet מתבצעת אך אילו קשיים שהתגברנו עליהם דיי מהר ותוך כדי עבודה הדברים הופנמו והובנו היטב.

היו פעמים גם שהרגשנו שאנחנו מתקדמות לאט יחסית כיוון בכל שלב היה לנו חשוב לוודא שאנחנו מבינות עד הסוף את מה שאנחנו עושות, גם אם זה היה על חשבון קצב ההתקדמות בפרויקט.

צורת העבודה הייתה חדשה לנו, מאתגרת, אך מליאת סיפוק!!!

אנחנו לגמרי מרגישות איך עלינו שלב בכמה היבטים שונים.

מבחינת הידע וההבנה, אני חושבת שהקורס הזה תרם לנו מאד. זה היה הקורס הראשון שלנו בכל הנושא של אבטחת מידע. זה פתח לנו אפיקים לתחום חדש שלא היכרנו. הרגשנו שרכשנו ידע רב בכל הנושא של קריפטוגרפיה, שיטות הצפנה, הכרה באיומים מפניהם יש להישמר, בנכסים עליהם אנו רוצים להגן ועוד.

מבחינת התכנות עצמו, נדרשנו לעבוד עם שתי שפות שונות בד בבד. אנחנו חושבות שהדברים הללו לחלוטין שפשפו אותנו ותרמו לנו מאד.

Future Work

הפרויקט הוא חלק ממערכת גדולה ומורכבת שניתן יהיה לפתח בהמשך. מובן שיש אינסוף דרכים לשכלל אותו ולפתח אותו בהיבטים שונים.

לדוגמא, היינו רוצות שעצם העברת המידע מהאפליקציה אל בסיס הנתונים של השב"כ תיעשה בצורה מוצפנת. להוסיף פונקציונליות ושאילתות נוספות שיכולות להיות רלוונטיות עבור קבלת המידע מבסיס הנתונים. מחיקת הנתונים של המשתמש באופן אבסולוטי אחרי עשרה ימים מיום האימות לקורונה, בדיקות ולידציה של הקלטים וכמובן הקפדה על חווית משתמש.

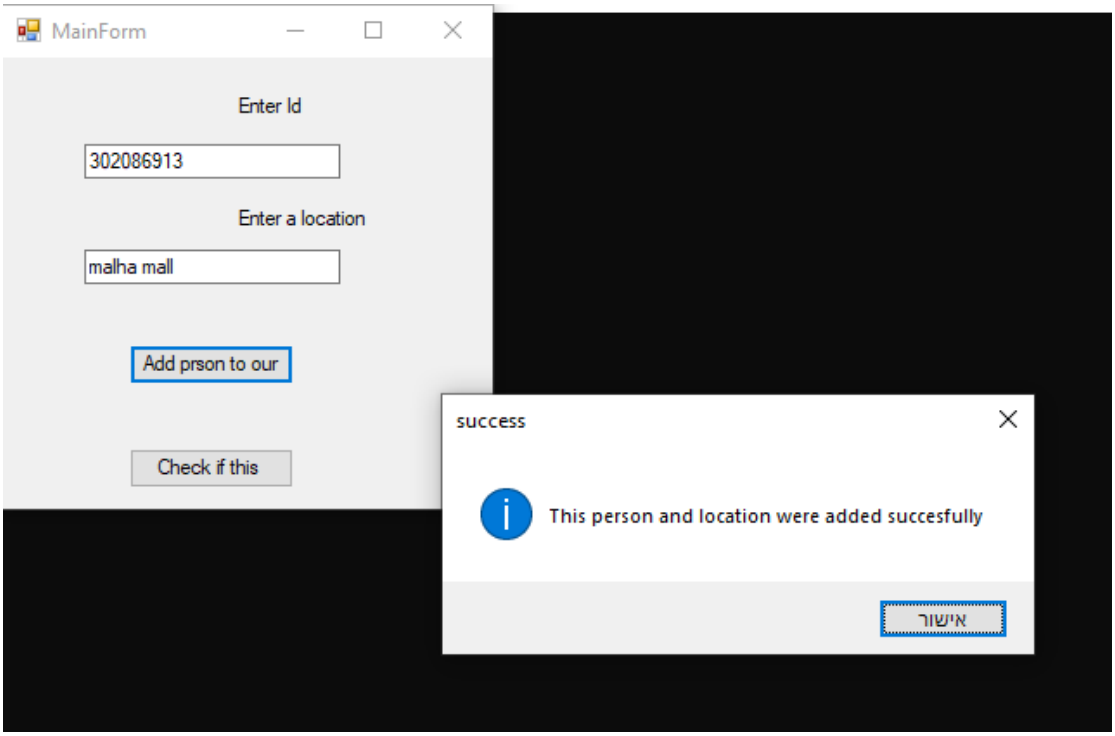
אנחנו לגמרי רואות את עצמינו ממשיכות לעבוד רבות על הפרויקט עד לקבלת מוצר מוגמר. אנחנו חושבות כי עצם המצאות מוצר כזה הוא חיוני ורלוונטי מאד במיוחד בימים אלו ואנחנו נשמח להמשיך ולפתח אותו.

How to Use the Project

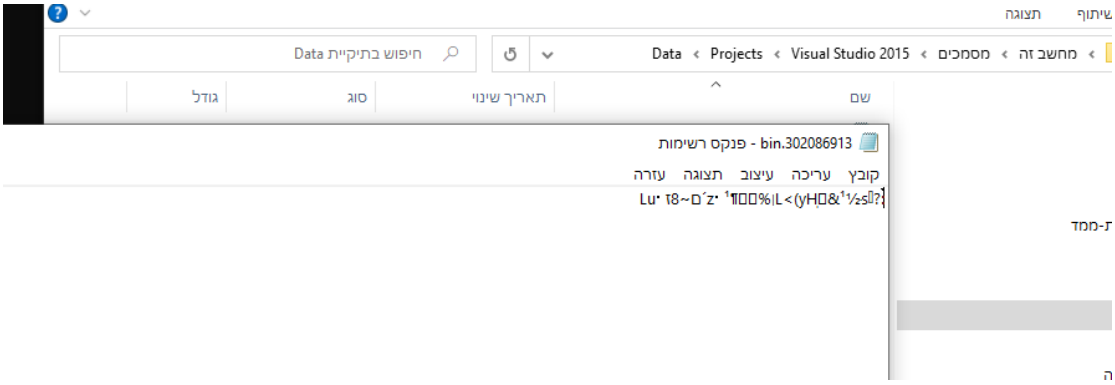
כאשר מריצים את הפרויקט TryTee יופיע החלון mainForm ובו שתי תיבות טקסט. בחלון זה יש שתי אפשרויות:

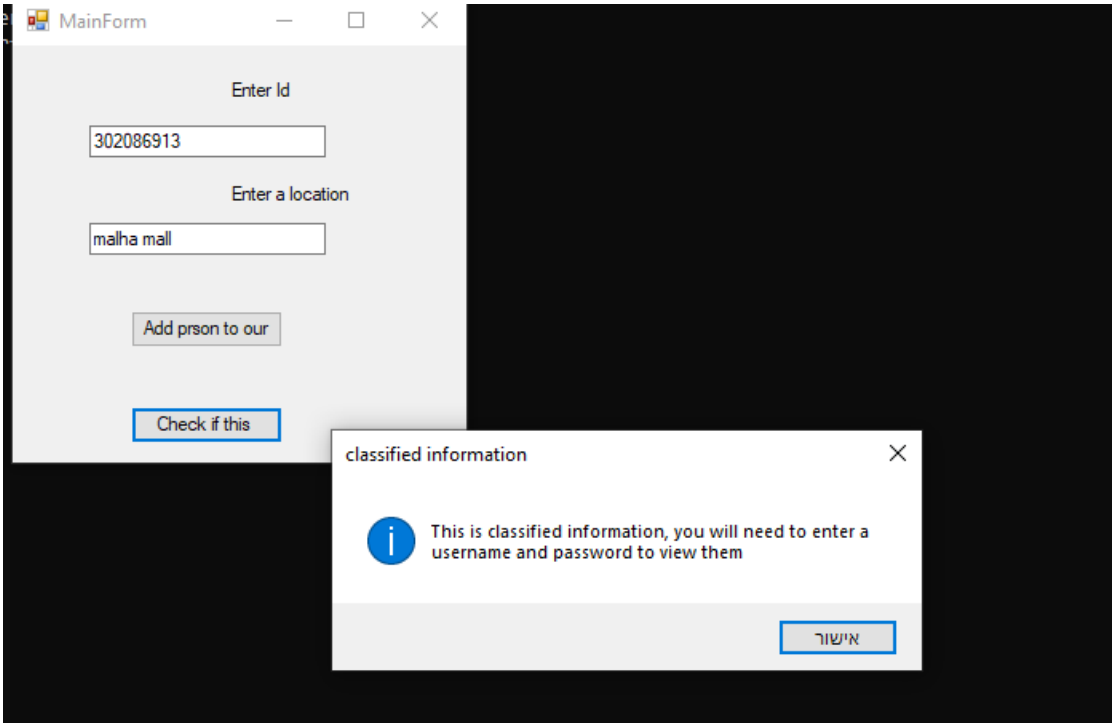
1. להוסיף עבור מספר זהות חדש, מיקומים בהם שהה.
2. לבדק האם מספר זהות מסוים שהה במיקום מסוים – כאשר נרצה לבצע בדיקה זו יפתח חלון חדש form1 המבקש שם משתמש וסיסמא כיון שנתונים אלו עשויים להיות רגישים ואיננו רוצים לחשוף אותם.

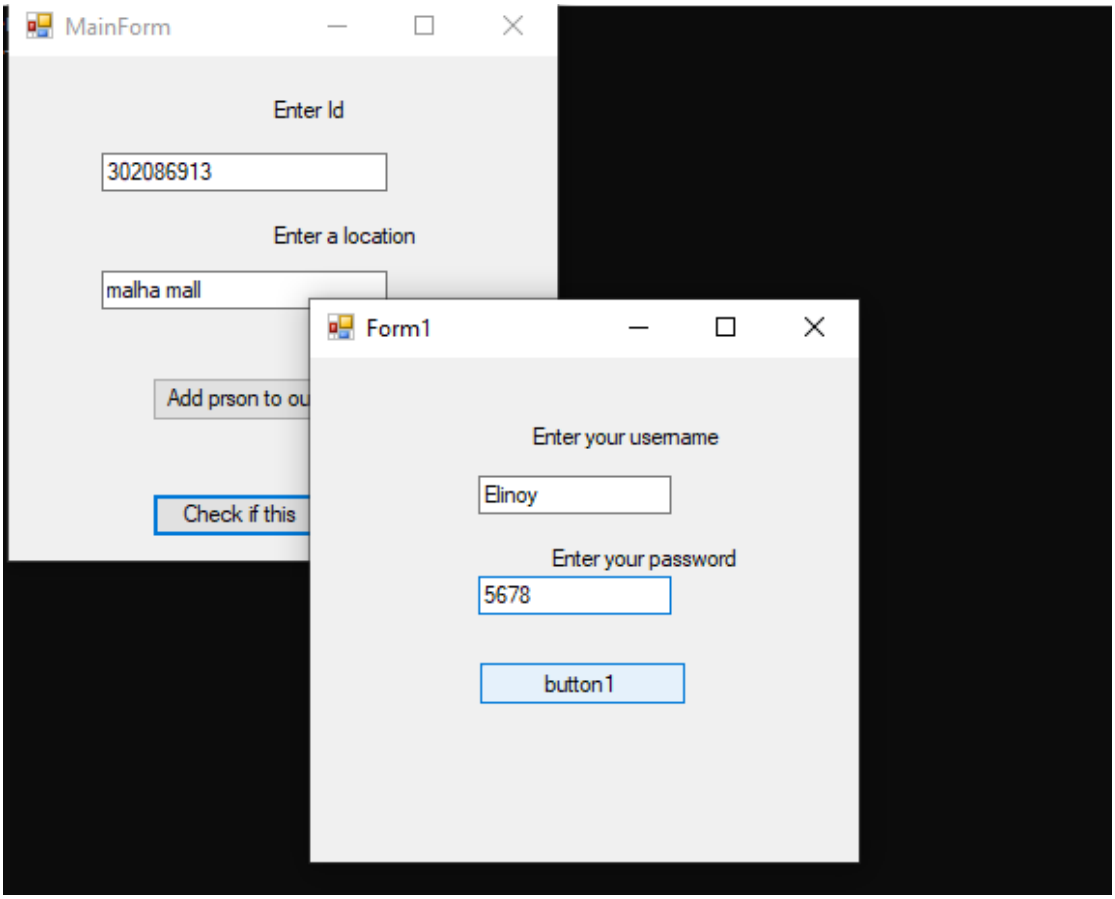
נוכל לראות בקבצים כי הנתונים אכן נשמרו בצורה מוצפנת ורק מי שהזין שם משתמש וסיסמא נכונים יוכל לבצע את השאילתה האם אדם X שהה במיקום Y. כל שלב בתוכנית מלווה ב message box מתאים.

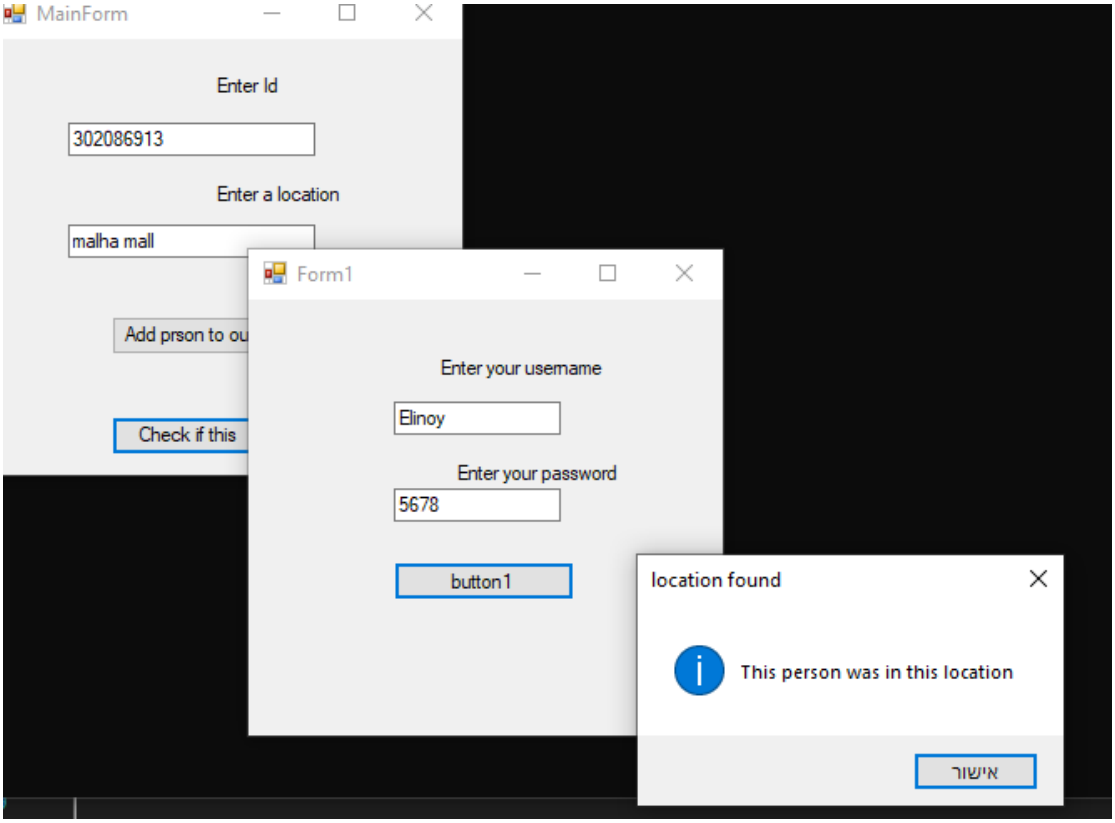


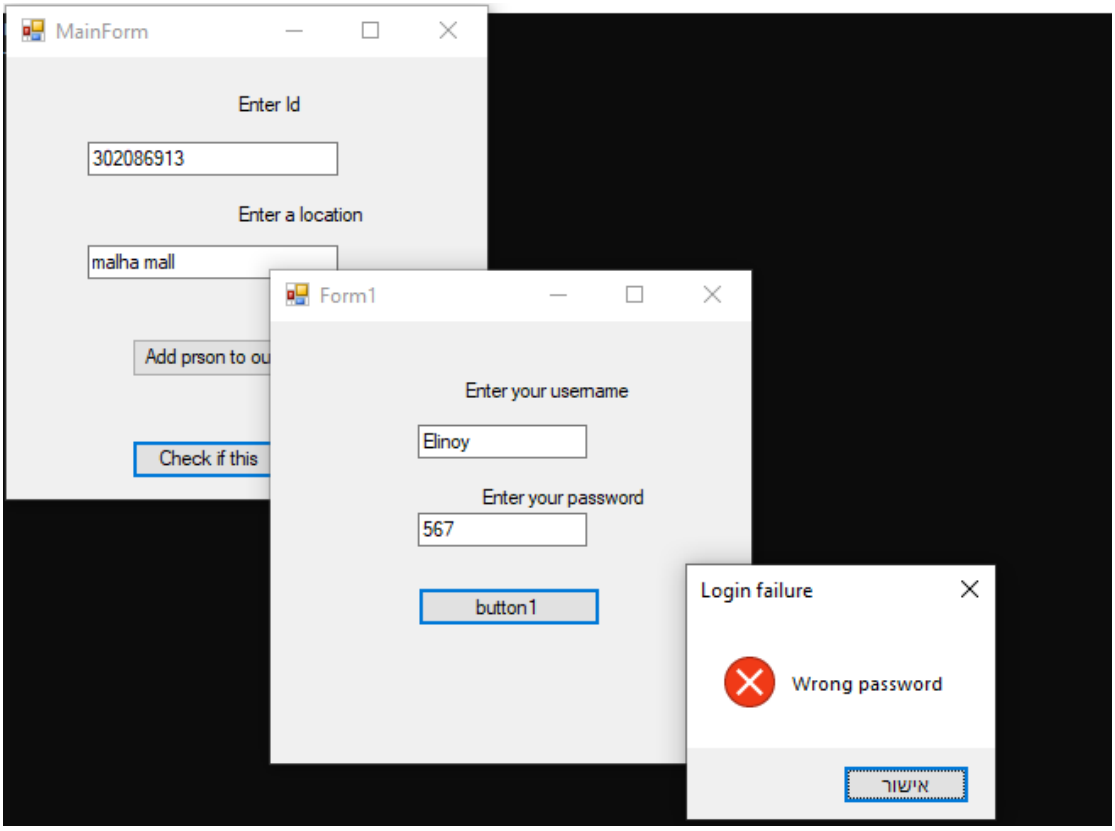
1 KB	קובץ BIN	10/03/2021 17:22	318252756.bin

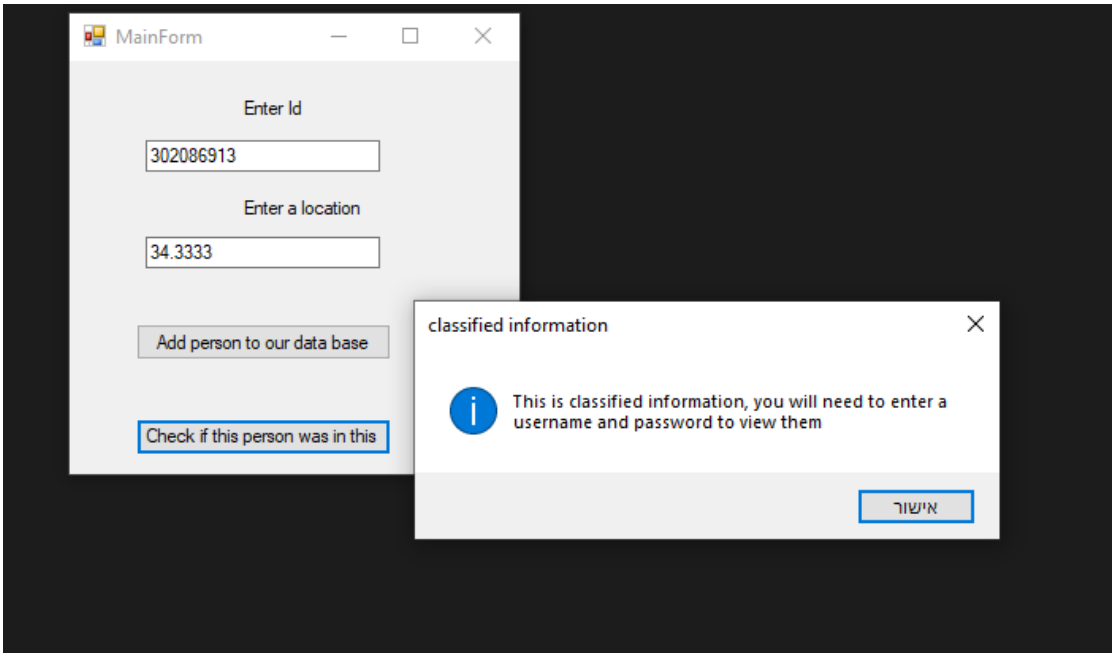


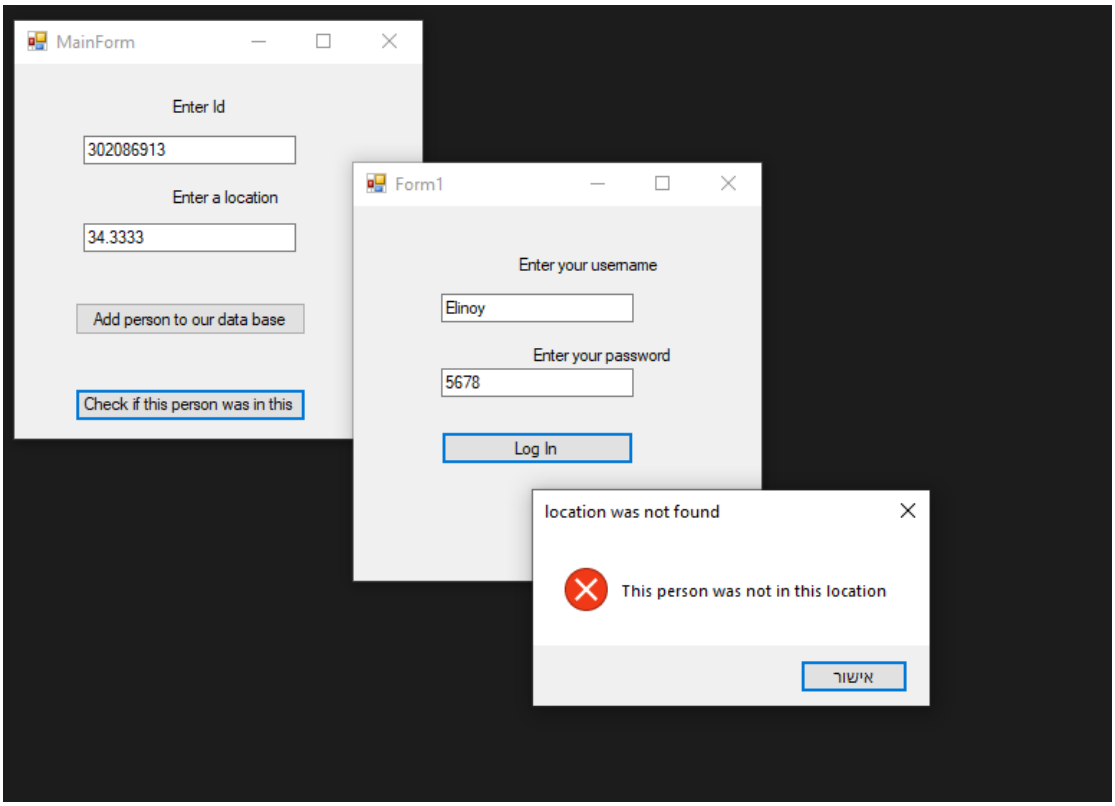

MainForm
Enter Id
302086913
Enter a location
malha mall
Add prson to our
Check if this
classified information
This is classified information, you will need to enter a username and password to view them
אישור

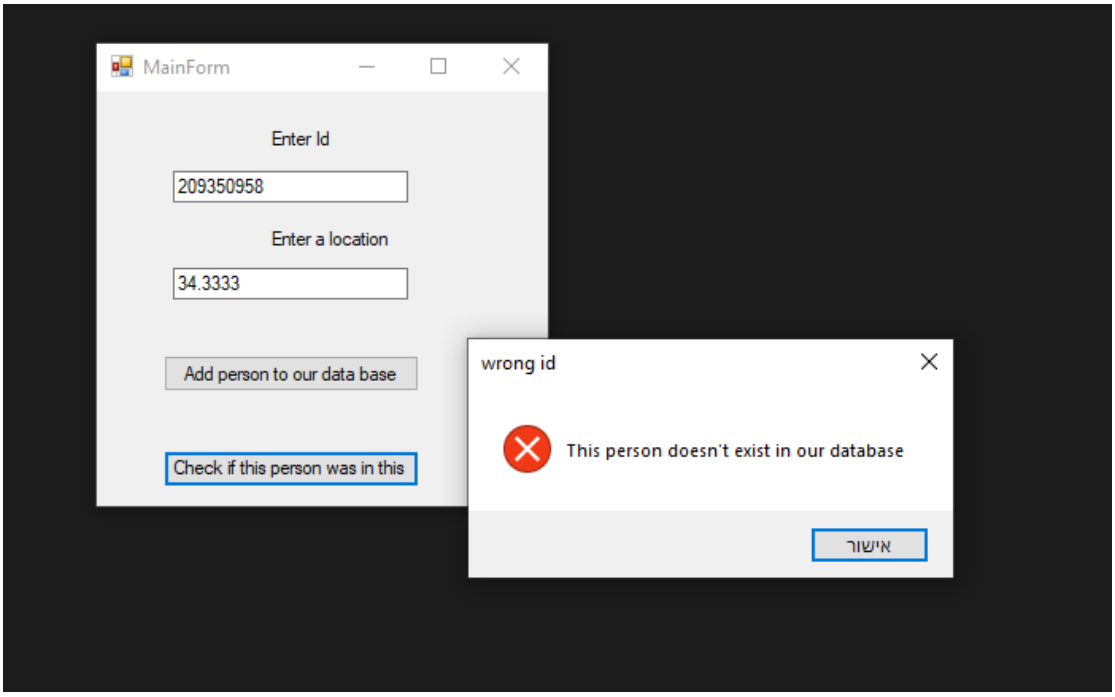

MainForm
Enter Id
302086913
Enter a location
malha mall
Add prson to ou
Check if this
Form1
Enter your usemame
Elinoy
Enter your password
5678
button1

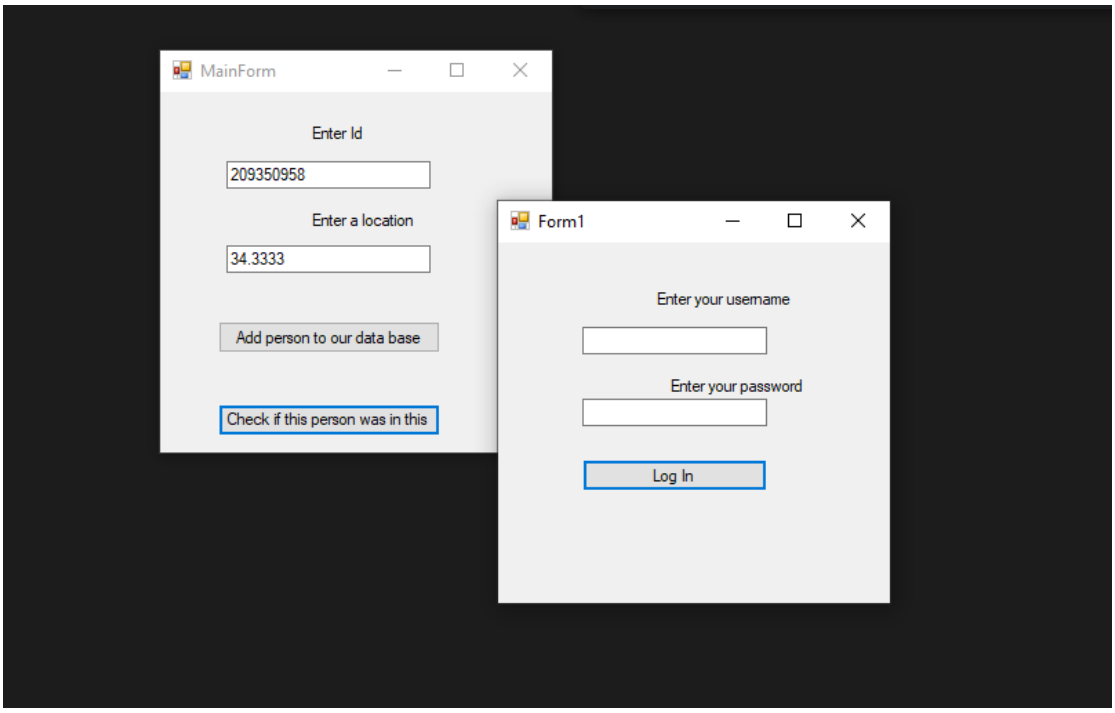

MainForm
Enter Id
302086913
Enter a location
malha mall
Add prson to ou
Check if this
Form1
Enter your usemame
Elinoy
Enter your password
5678
button1
location found
This person was in this location
אישור


MainForm
Enter Id
302086913
Enter a location
malha mall
Add prson to ou
Check if this
Form1
Enter your usemame
Elinoy
Enter your password
567
button1
Login failure
Wrong password
אישור


MainForm
Enter Id
302086913
Enter a location
34.3333
Add person to our data base
Check if this person was in this
classified information
This is classified information, you will need to enter a username and password to view them
אישור


MainForm
Enter Id
302086913
Enter a location
34.3333
Add person to our data base
Check if this person was in this
Form1
Enter your username
Elinoy
Enter your password
5678
Log In
location was not found
This person was not in this location
אישור


MainForm
Enter Id
209350958
Enter a location
34.3333
Add person to our data base
Check if this person was in this
wrong id
This person doesn't exist in our database
אישור


MainForm
Enter Id
209350958
Enter a location
34.3333
Add person to our data base
Check if this person was in this
Form1
Enter your username
Enter your password
Log In