האוניברסיטה הפתוחה
המחלקה למתמטיקה ולמדעי המחשב
החטיבה למדעי המחשב

פרויקט מתקדם במדעי המחשב:
אבטחת תקשורת בין רכבית מימוש והדגמה של אלגוריתם אימות הרכב במידע מחוץ לרשת.

מנחה: פרופ' אהוד גודס

מגיש:
ספי צמח
ת.ז. 036412930

סמסטר ב' 2019

פרויקט מתקדם זה הוגש כחלק מהדרישות לקבלת תואר "מוסמך (M.Sc.) במדעי המחשב"

באוניברסיטה הפתוחה

ינואר 2019

תוכן עניינים

1. גרסאות המסמך 5
2. מטרת הפרויקט 6
3. מבוא 6
א. תיאור הבעיה 6
ב. תיאור התקפת MitM 7
4. תיאור האלגוריתם והפרוטוקול המוצע 9
א. שלב היצירה 9
ב. שלב החתימה 9
ג. יצירת ההקשר והחלפת המפתחות 9
ד. שליחת הודעה מוצפנת 10
ה. התקפות על הפרוטוקול המוצע 10
5. תיאור הפרויקט 13
6. מפרט דרישות תוכנה (SRS) 16
א. הנחות והגדרות 16
דימוי תקשורת אלחוטית 16
דימוי זיהוי פיזי על ידי חיישנים – Out of Bound 17
ב. דרישות 18
ג. ממשק משתמש כללי 20
7. כלים ושפת פיתוח לביצוע הפרויקט 21
8. מימוש הפרויקט 22

א. הפרויקט Vehicle 22

ב. הפרויקט General 30

ג. הפרויקט Certification Authority 31

ד. הפרויקט QRCodeCraetor 33

9. תוצאות 34

א. הקמת ערוץ תקשורת חתום על ידי CA תסריט תקין 34

ב. הקמת ערוץ תקשורת חתום על ידי CA תסריט התקפת MitM 35

ג. הקמת ערוץ תקשורת חתום על ידי CA כולל אימות Out of band תסריט התקפת ניגון מחדש של הודעות עבר 39

10. מסקנות / סיכום 42

11. רשימת מקורות 43

12. נספחים 44

א. מסכי אפליקציות ומדריך שימוש 44

מסכי אפליקציית Vehicle 44

מסכי אפליקציית Attacker 46

מסכי אפליקציית Certificate Authority 47

מסכי אפליקציית Out Of Band Visual sign (QR Code) Creator 48

רשימת איורים

איור 1 : MitM Diffie Hellman 7
איור 2 : מבנה תעודה אופיינית (דוגמה)..... 9
איור 3 : תיאור הפרוטוקול המוצע 10
איור 4 : דוגמת תקיפה א' - הקלטת השיחה 11
איור 5 : דוגמת תקיפה ב' הקלטת השיחה..... 12
איור 6 : דוגמת תקיפה ב' הקלטת השיחה..... 12
איור 7 : דוגמת תקיפה ב' התקפה על בסיס הקלטת השיחה..... 13
איור 8 : הקמת תקשורת תקינה 14
איור 9 : התקפת האדם שבתווך 14
איור 10 : אימות רכב על פי הפרוטוקול המוצע (Out of Band)..... 15
איור 11 : אימות רכב על פי הפרוטוקול המוצע – כישלון התקפה 15
איור 12 : כתובות רשת לדוגמא במחשב המדגים 17
איור 13 : דרישות ממשקי משתמש 20
איור 14 : פעילויות אפשריות במערכת ההדגמה..... 21
איור 15 : סוגי הודעות אפשריות 23
איור 16 : מבנה נתונים של הודעות התקשורת..... 23
איור 17 : תרשים זרימה (החלפת מפתחות נאיבית)..... 24
איור 18 : תרשים זרימה החלפת הודעות עם וידוא כפול OutOfBand..... 25
איור 19 : תרשים זרימה תצורת תוקף (התחזות והקלטה) 27
איור 20 : המחלקה Vehicle..... 29
איור 21 : חתימת CA על פרטי רכב..... 32
איור 22 : ממשק משתמש אפליקציית Vehicle..... 45
איור 23 : ממשק משתמש אפליקציית Vehicle פקודות נוספות 45
איור 24 : ממשק משתמש אפליקציית Attacker 46
איור 25 : ממשק משתמש אפליקציית Attacker הקלטה וניגון הודעות..... 47
איור 26 : ממשק משתמש אפליקציית Certificate Authority 47
איור 27 : ממשק משתמש אפליקציית Visual Sign creator..... 48

1. גרסאות המסמך

מס' גירסה	שינויים
1.0	טיוטה ראשונה
1.1	תיקונים לאחר הערות המנחה

2. מטרת הפרויקט

מטרת הפרויקט היא לממש ולהדגים את האלגוריתם והפרוטוקול שפיתחו : Shlomi Dolev Michael Segal, Lukasz Krzywiecki , Nisha Panwar, המתואר ב-[1]. האלגוריתם הינו שיטה לאימות רכבים איתם מקיימים תקשורת אלחוטית, השיטה מגנה בפני התקפות MITM בה גורם אשר נמצא בתווך התקשורת מאזין לשלב הקמת הקשר ועל ידי כך יכול בשלב מאוחר יותר להתערב ולשבש את התקשורת בין הרכבים מבלי להתגלות. השיטה מבוססת אימות מחוץ לרשת (Out of Band) של רכיב הניתן לאימות/זיהוי על ידי חיישן קורא כלשהו למשל : לוחית המכילה מספר רישוי הניתן לזיהוי על ידי מצלמה, אשר ייצוגו מוטמע בהודעת תקשורת מאומתת וחתומה. על ידי הצלבת הנתונים מתבצע אימות כפול של הרכב המשדר.

3. מבוא

מכונית אוטונומית היא מכונית המנווטת בעצמה ומתגברת על מכשולים ללא עזרה של נהג אנושי. המכונית האוטונומית צפויה להיות בטיחותית יותר והנסיעה בה יעילה וחסכונית יותר. בשיטות נהיגה אוטונומית מתקדמות הרכבים מתקשרים ביניהם באמצעות תקשורת בין רכבית (Vehicular network) על מנת לקבל מידע על הרכבים הסובבים אותם, וזאת על מנת להגביר בטיחות, לחסוך במשאבים ולהקטין זיהום אוויר [2-3] .

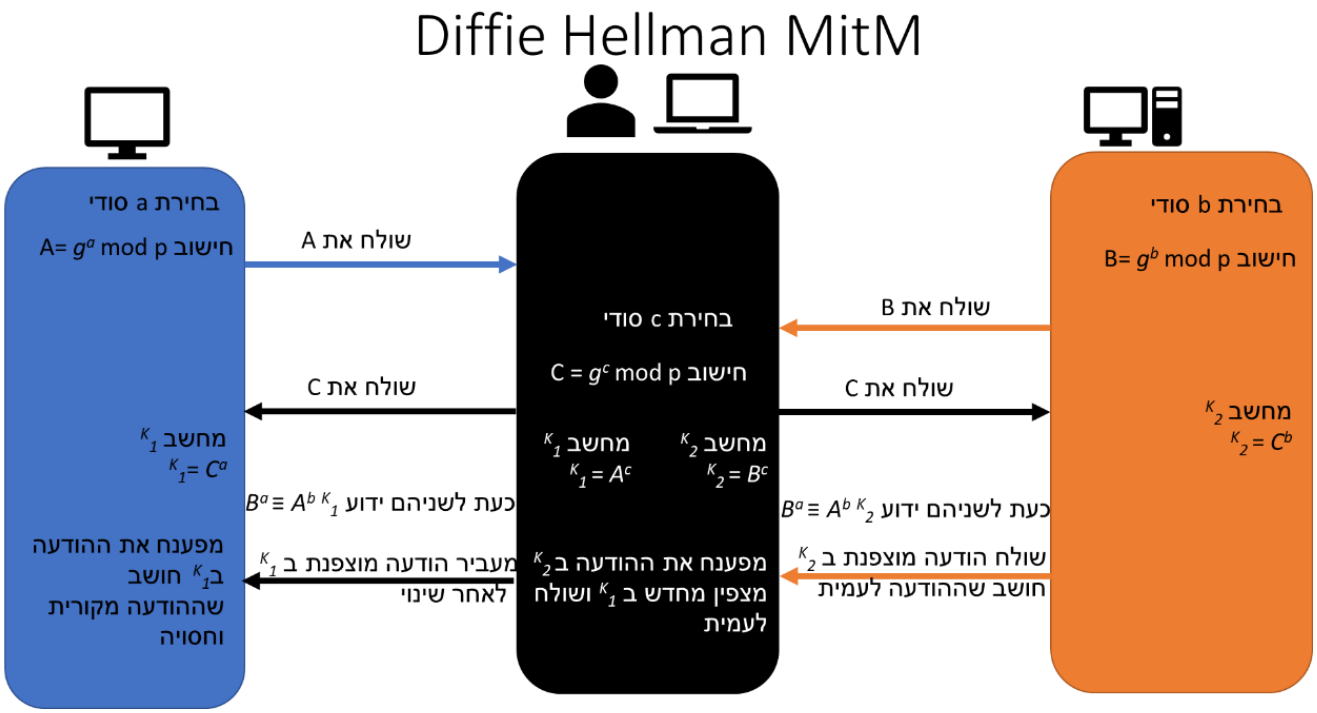
רשתות בין רכביות משמשות לשיתוף פעולה בין רכבים באמצעות משדרי ומקלטי RF, למרבה הצער השידור האלחוטי פגיע אל מול איומי אבטחה אשר להן משמעויות בטיחותיות קשות.
ובכללן התמודדות עם איום- MitM Man in the Middle האדם שבתווך.
בדרך כלל במקרים אלו אחד הפתרונות הוא תקשורת מבוססת מפתח ציבורי אשר מאושר על ידי רשות אישור (CA - Certification Authority) שמונעת אפשרות לשלוח הודעות חדשות בשם שולח מסוים, שיטה זו לא תמנע התקפות כגון התחזות.

א. תיאור הבעיה

בסוג התקשורת לו אנו מייעדים את שיפור האבטחה יש שימוש במפתח ציבורי ופרטי.
בדרך כלל מפתחות ציבוריים נחתמים ע"י רשות אישור אשר ניתנת לזיהוי ע"י המקבל, ברשתות זמניות (Ad-hoc) אשר חבריה מצטרפים ועוזבים תדיר אין אפשרות בעקבות הצורך בחיבור מהיר מאוד לערב בתקשורת גורם מאשר צד שלישי אשר יכול לאשר בזמן אמת את החבר המצטרף.

ללא שימוש בתקשורת עם רשות אישור Certification authority CA התקשורת הנ"ל חשופה להתקפות MitM.

ב. תיאור התקפת MitM



איור 1 : MitM Diffie Hellman

פרוטוקול Diffie Hellman מאפשר החלפת מפתחות בין 2 ישויות אשר אין להם שיתוף מידע מקדים להעביר אחד לשני מעל גבי ערוץ פתוח מפתח כך שאיש מלבדם אינו יודע מהו ובאמצעותו להצפין מידע ולהעבירו בערוץ פתוח . מכיוון שאין שימוש באימות על פי גורם צד שלישי אזי תוקף יכול ליירט את התשדורת, להתחזות לאחד או לשני הצדדים ולתקשר במקומם בשלב תהליך החלפת המפתחות. בדרך זו יכול התוקף לתקשר עם 2 הישויות הלגיטימיות להעביר הודעות מאחד לשני תוך כדי ציטוט או שינוי המידע כמתואר באיור 1.

אחד הפתרונות המוצעים להתמודדות עם הבעיה הוא על ידי זיהוי מחוץ לרשת (Out of Band) הנ"ל יתבצע בעזרת צימוד של מפתח ציבורי ורשימת מאפיינים ניתנים לזיהוי על ידי סנסורים כדוגמת מצלמה, מיקרופון , טביעת אצבע של משדר אלחוטי .

בשיטה משולבת זו בעלי רכבים מחויבים להליך קדם להליך התקשורת אשר מאשר/מספק מפתח ציבורי וכן מאשר מס' מאפיינים אשר ניתנים לזיהוי על סנסורים חיצוניים.
הנתונים כמקשה אחת יאומתו פיזית על יד CA בשלב מוקדם ויחתמו.
בזמן החלפת המפתחות, יתבצע אימות כפול – הן של החתימה והן של הזיהוי הפיזי.

4. תיאור האלגוריתם והפרוטוקול המוצע

א. שלב היצירה

כל רכב יחזיק תעודה דיגיטלית אשר מכילה פרטי זיהוי המתארים אותו כגון מס' רישוי , סוג רכב, צבע וכו', ראה דוגמא לתעודה אופיינית באיור מס' 2. התעודה תכיל גם את המפתח הציבורי של הרכב.

World Manufacturer Identifier (geographic area, country, plant code)	
Vehicle Descriptor Section (model year, brand logo, body style, original color and texture, color repairs, roof racks, foot step, mud flap, front and rear guard)	
Vehicle Indicator Section (engine number, engine type, license number, chassis number)	
GPS Device Identification	Wireless Device Fingerprint
Procedures to Execute for Verifying the Attributes	
Certificate Sequence Number	Certificate Expiration Date
Public Key	
Digital Signature	

איור 2: מבנה תעודה אופיינית (דוגמה)

ב. שלב החתימה

בכל תקופת זמן תחתם התעודה הדיגיטלית על ידי Certificate Authority באמצעות מפתח פרטי. המפתח הציבורי יופץ וניתן יהיה לוודא כי התעודה חתומה והרכב זוהה על ידי גורם מוסכם (המאמר מעלה אפשרות שגורם מוסכם זה יהיה ממשלתי – כגון משרד הרישוי).

ג. יצירת הקשר והחלפת המפתחות

כאשר רכב א' מעוניין ליצור קשר עם רכב ב'
הוא שולח לו את התעודה הדיגיטלית והמפתח הציבורי + חתימה על התעודה שקיבל ממשרד הרישוי

$$CertS = AttributeS + Public\ keyS || SignCA(H(AttributeS + Public\ keyS))$$

רכב ב' מוודא חתימה על ידי הרשות CA
מוודא כי המאפיינים הכתובים בתעודה מתאימים למידע הוויזואלי של הרכב עצמו
שולח תעודה חתומה משל עצמו

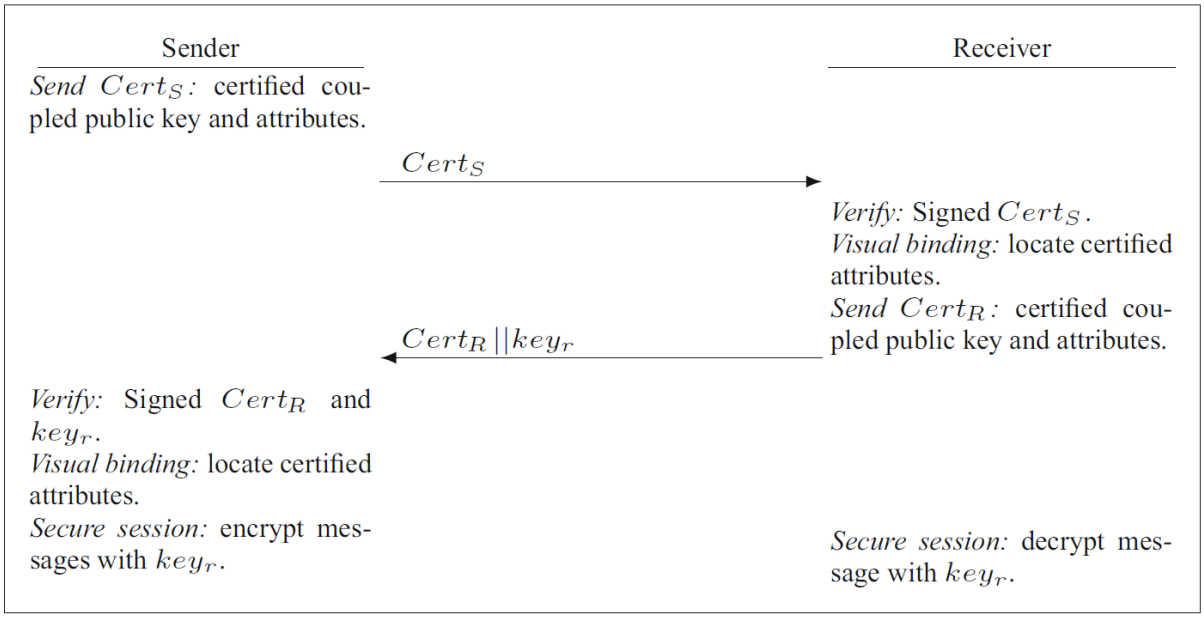
$CertR = AttributeR + Public\ keyR||SignCA(H(AttributeR + Public\ keyR))$
ומפתח שיחה מוצפן עם מפתח ציבורי של א'

$EPublic\ keyS\ (keyr + Seq.Num.S)||EPublic\ keyS\ (ESKR(H(keyr + Seq.Num.S)))$
וחתום ע"י מפתח פרטי של ב'.

רכב א' מקבל את התעודה של רכב ב' מוודא חתימה של CA ,
מוודא כי המאפיינים הכתובים בתעודה מתאימים למידע הוויזואלי של הרכב עצמו .
שלבי ההחלפה מתוארים גם באיור מס' 3.

ד. שליחת הודעה מוצפנת

המפתחות הוחלפו כעת הרכבים יכולים לנהל שיחה מוצפנת



איור 3 : תיאור הפרוטוקול המוצע

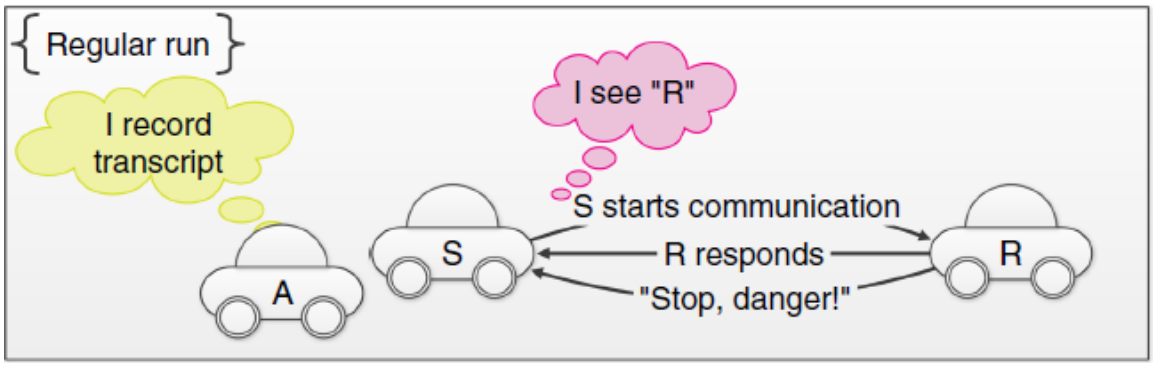
ה. התקפות על הפרוטוקול המוצע

תקיפה מסוג א' : התחזות לשולח
נניח כי תוקף נמצא במרחק שידור רדיו משולח הודעות S בעל מאפיינים Attributes
וממקבל הודעות R בעל מאפיינים ,Attributer

התוקף מקליט הודעות מ S כולל שידור התעודה המאושרת שלו על מנת שיוכל לנגן הודעות אלו ולהתחיל שיחה עם אחרים בהתחזות ל S .
למרות שהתוקף לא יוכל לפתוח הודעות שישלחו אליו בחזרה שכן המפתח הציבורי בהודעות המשודרות שייך ל S ולתוקף אין את המפתח הפרטי.
ההתקפה יכולה לנסות לבלבל את R בחושבו כי S מעוניין לשוחח איתו .
כך ש R בוחר מפתח שיחה ומשדר הודעות מוצפנות באמצעותו.

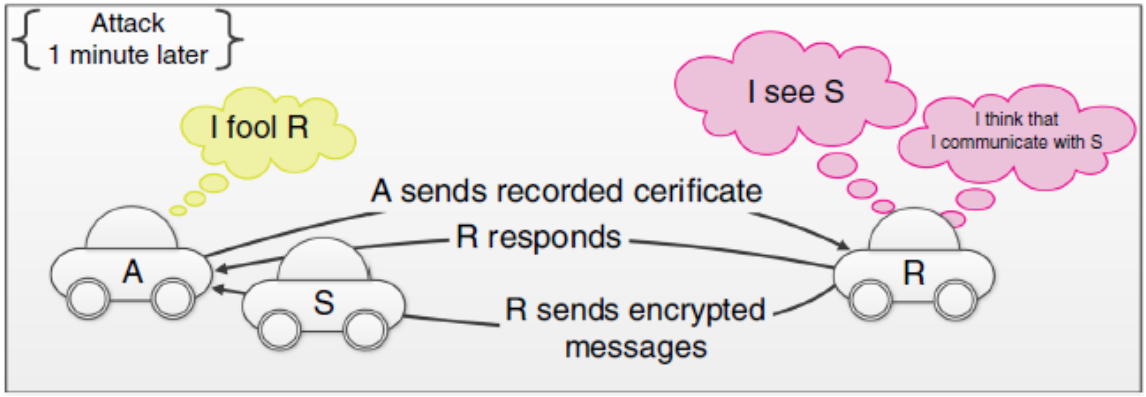
נדגים : ניסיון התקפה על בסיס ההקלטה

שלב א' הקלטת השיחה ראה איור מס' 4.



איור 4 : דוגמת תקיפה א' - הקלטת השיחה

שלב ב' ניגון מחדש של חלקים מהשיחה המוקלטת ראה איור מס' 5.

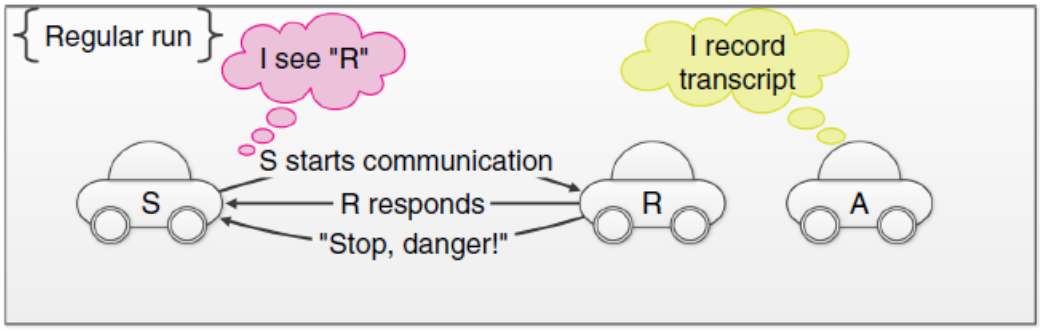


איור 5 : דוגמת תקיפה ב' הקלטת השיחה

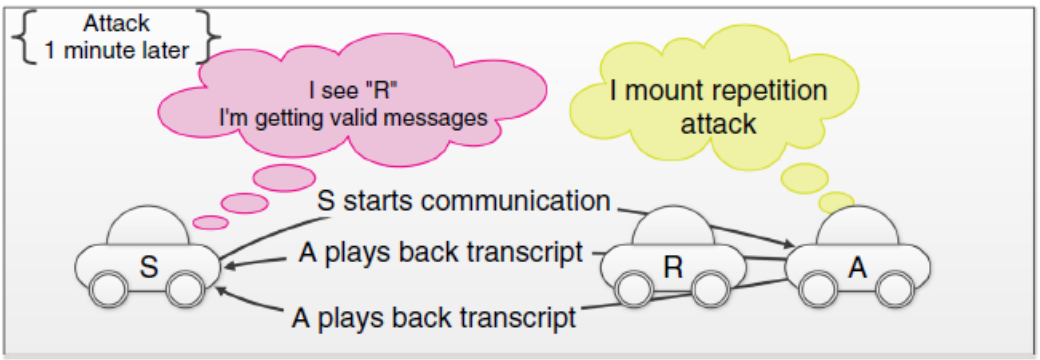
ההתקפה חייבת להתבצע כאשר רכב S עדיין באזור שכן ללא נוכחותו R לא יכול לאמת את המאפיינים שלו, ולא ישלח הודעות מוצפנות.

התמודדות מול התקיפה
ניתן להגן ע"י הוספה של הודעת Ack מוצפנת ששולח S בסיום התהליך כך R לא ישלח הודעות מוצפנות מיד לאחר בחירת מפתח השיחה אלא יחכה לאישור מ S על קבלתו – אישור זה יכול להישלח רק ע"י S , ולכן R לא ישלח הודעות מוצפנות.

תקיפה מסוג ב' : התחזות למקבל
התוקף מקליט הודעות מ S (ראה איור מס' 6) וכן מענה של הודעות מ R כולל שידור התעודה המאושרת שלו על מנת שיוכל להתחזות ל R ולענות במקומו במידה ו S יפנה אליו שוב .
S יחשוב שהוא משוחח עם R אך מי שיקבל את ההודעות יהיה התוקף (ראה איור מס' 7) .
מכיוון ש S קיבל את המפתח בהודעה המוקלטת הראשונה התוקף יכול להמשיך לשלוח הודעות מוקלטות מהעבר S יקבל אותן כהודעות חוקיות, יפתח אותן ויעבוד עם המידע המתקבל כמידע לגיטימי, כך התוקף יכול להזין את S במידע שגוי .



איור 6 : דוגמת תקיפה ב' הקלטת השיחה



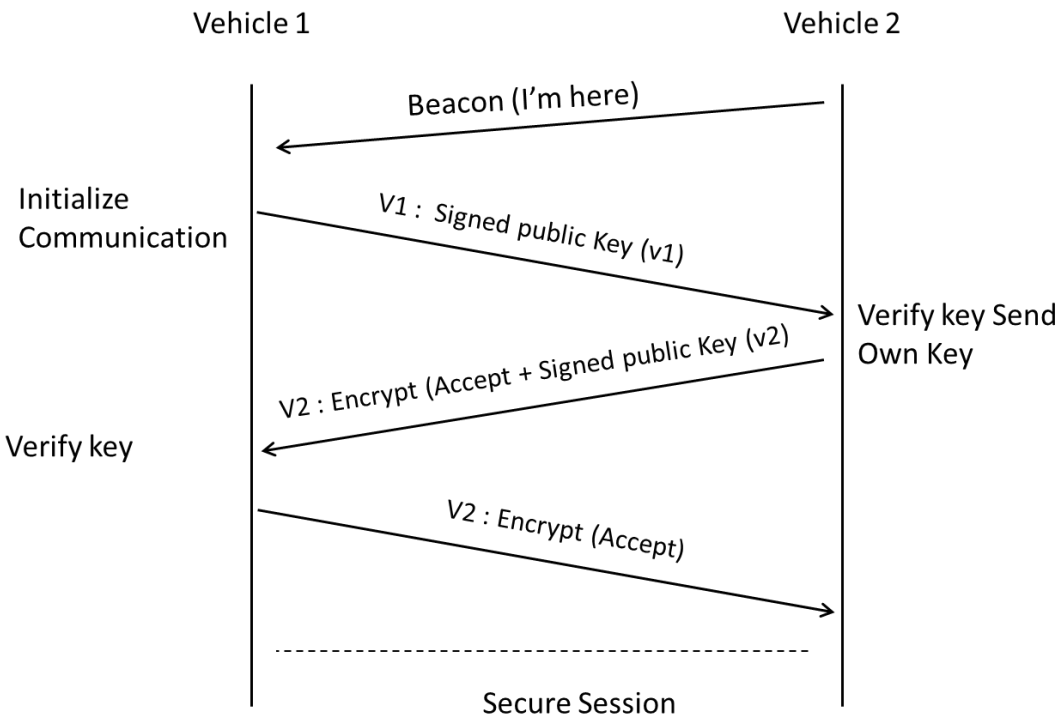
איור 7 : דוגמת תקיפה ב' התקפה על בסיס הקלטת השיחה

5. תיאור הפרויקט

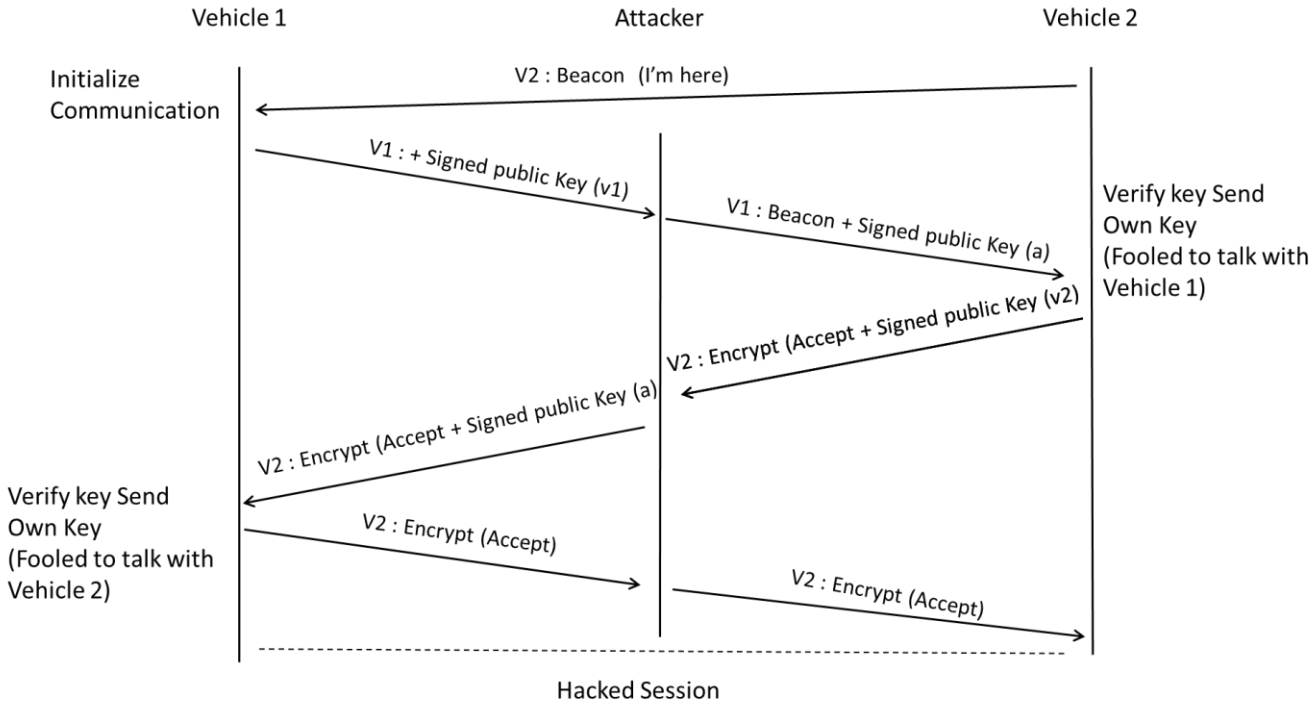
הרעיון שבבסיס הפרויקט הינו לממש אפליקציות אשר מדמות התנהגות תקשורת רכבים בתקשורת UDP/IP כל אפליקציה תדמה רכב הנוסע בדרך, ומתקשר עם הסביבה בצורה מאובטחת על ידי שימוש במפתח פרטי וציבורי. תיבנה אפליקציית תקיפה אשר תאזין לתקשורת ותבצע תקיפה MitM. הפרויקט ידגים אבולוציה של פתרונות אבטחה ושכלול ניסיון תקיפה.

הפרויקט מדגים מספר תסריטים :

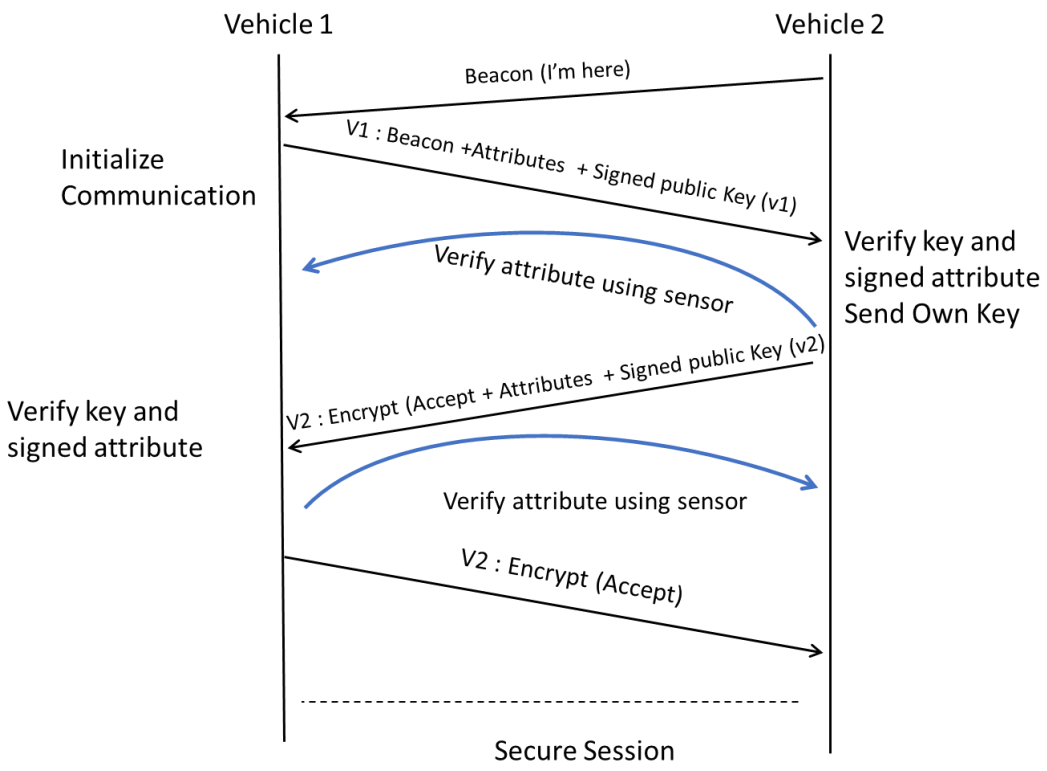
- תקשורת תקינה בין 2 רכבים על ידי שימוש במפתח ציבורי ופרטי והעברתם בפרוטוקול דיפי הלמן [5] ולאחריו החלפת מידע מוצפנת (ראה איור מס' 8)
- התקפה MitM ע"י תוקף וביצוע שינוי נתונים (ראה מס' איור 9)
- שימוש באימות מפתח ע"י תוכנה נוספת CA ועל ידי כך להתמודד עם ההתקפה
- שימוש בשיטה המודגמת במאמר לשילוב מזהים סטאטיים של הרכב בנתונים החתומים ועל ידי כך להתמודד עם ההתקפה (ראה איורים מס' 10 ו 11)
- התקפת ניגון מחדש של נתוני עבר ע"י המתקיף (מתואר בפירוט בפרק 4. סעיף ה.)



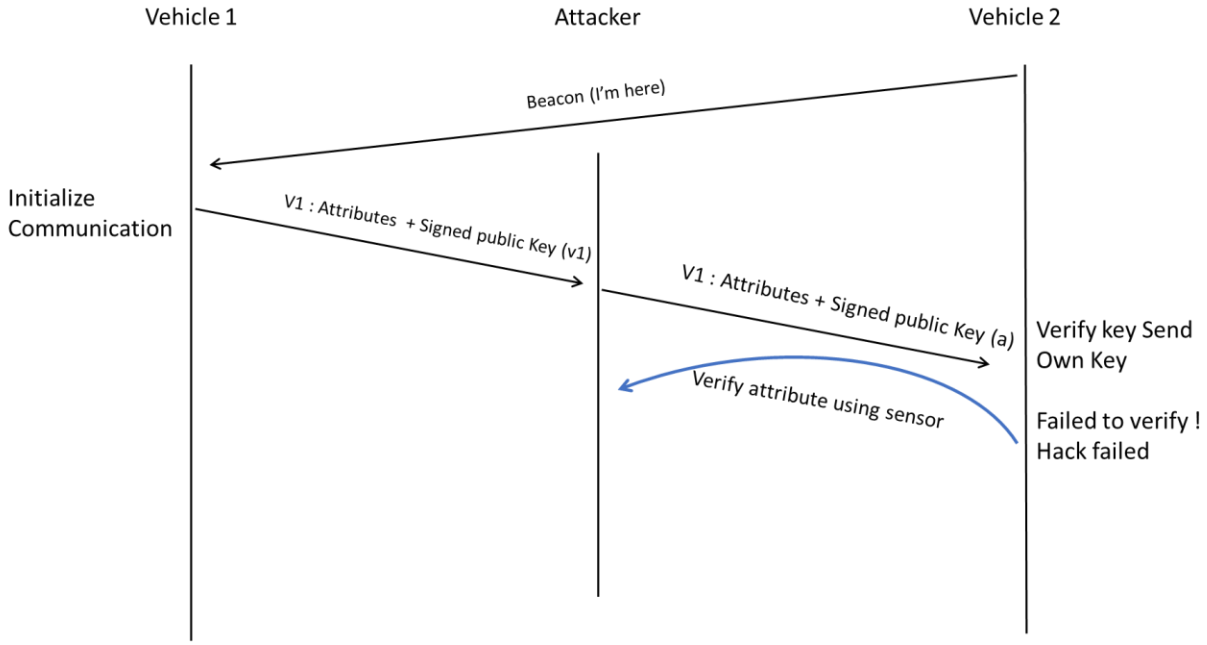
איור 8 : הקמת תקשורת תקינה



איור 9 : התקפת האדם שבתווך



איור 10 : אימות רכב על פי הפרוטוקול המוצע (Out of Band)



איור 11 : אימות רכב על פי הפרוטוקול המוצע – כישלון התקפה

6. מפרט דרישות תוכנה (SRS)

א. הנחות והגדרות

דימוי תקשורת אלחוטית

רקע : תקשורת Unicast ו Multicast

Unicast

היא תשדורת בין רשתות מנקודה אחת לנקודה מסוימת אחרת וזאת על פי זיהוי של הכתובת, לכל ישות ברשת יש כתובת ייחודית ובמידה ושולחים הודעה עם כתובת היעד הספציפית, ישויות רשת אחרות עם כתובת שונה יתעלמו מההודעה הנ"ל ורק בעל בכתובת יקרא/יעבד אותה.

לדוגמה מחשב א' מתחבר לשירות FTP והורדת קבצים סוג התשדורת הוא Unicast כיוון שהשרת FTP שולח את המידע לישות ספציפית אחת. השימוש בו הוא ליצור חיבור פרטי בין 2 הנקודות.

טווח הכתובות של Unicast זה 0.0.0.0 ל 223.255.255.255.255 מתוכם כמובן סוג תקשורת זה נקרא גם one-to-one .

Multicast

היא תשדורת מנקודה אחת לכמה נקודות ,זאת אומרת שליחה בתשדורת אחת (חיבור אחד) את המידע לכמה מחשבים בו זמנית וזאת על ידי פרוטוקול UDP .

כל ישויות הרשת אשר מבקשות לקבל את המידע המופץ נרשמות לכתובת הנ"ל, הודעה אשר תשלח לכתובת הנ"ל תקרא/תעובד על ידי כל ישויות הרשת אשר נרשמו לכתובת ללא קשר לכתובת הרשת הפרטית שלהן.

הסיבה שישתמשו ב Multicast היא למנוע כמה שפחות חיבורים נפרדים לצורך העברת מידע זהה, סוג תקשורת זה נקרא גם one-to-many

טווחה כתובות הוא 224.0.0.0 עד ל239.255.255.255 .

מימוש : שימוש ב Multicast בפרויקט זה

תקשורת בין רכבית משתמשת בתווך אלחוטי על מנת להעביר הודעות בין הרכבים, בתקשורת אלחוטית כל הודעה נשלחת באוויר ועשויה להיקלט על ידי משתמשים שונים

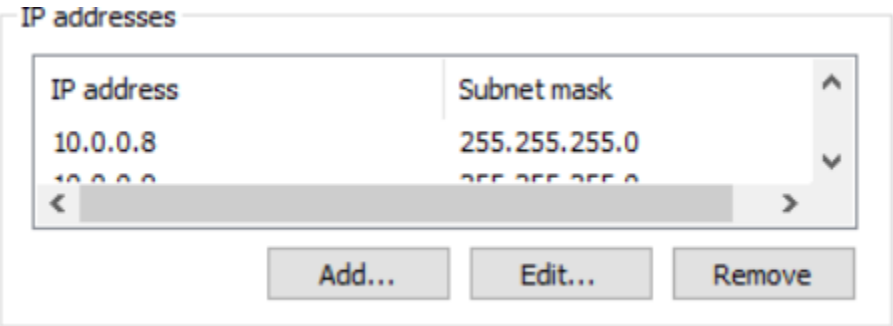
ועקב כך להיות חשופה להתקפת MitM.

פרויקט זה נדרש להדגמה פשוטה ועל מחשב אחד אם ניתן.

על מנת לדמות תקשורת בתווך אלחוטי אך עדיין לבדוק ולהדגים הנ"ל בקלות על מחשב אחד כמספר משתמשים בו זמנית, נבחר פתרון של תקשורת Multicast כדרך התקשורת העיקרית. כלומר כאשר אפליקציה שולחת הודעה למשתמש מסוים, היא שולחת אותו ליעד Multicast כך כל האפליקציות האחרות יכולות להקשיב לו – בדומה להודעה אשר נשלחת בתווך אווירי. היעד האמתי נשלח בתוך שדה בהודעה ומאפשר לאפליקציית היעד לסנן על פיה ולהתחשב בהודעות המגיעות אליה בלבד מחד ולאפשר לאפליקציית תקיפה להקשיב להודעות כאילו עברו בתווך אווירי ולייירט אותן.

כל האפליקציות המשתמשות ביכולות תקשורת (Attacker,Vehicle) מאזינות לאותה כתובת Multicast.

לצורך שליחת הודעה לכל אפליקציה יש כתובת IP ייעודית במחשב.



איור 12 : כתובות רשת לדוגמא במחשב המדגים

במקרה המודגם כאן, מוגדרות 3 כתובות רשת (1.0.0.7,1.0.0.8,1.0.0.9) כמודגם באיור מס' 12.

שתיים עבור אפליקציות Vehicle ואחת עבור אפליקציית Attacker.

דימוי זיהוי פיזי על ידי חיישנים – Out of Bound

שיטת הזיהוי OutOfBand

שיטת הזיהוי הנזכרת לעיל משתמשת בחיישנים על מנת לקלוט מזהים של הרכב מתקרב ובכך לזהות אותו וכן לוודא שהוא נמצא בטווח קרוב.

על מנת לדמות אימות בקריאה של נתונים Out Of Band נשתמש במנגנון כתיבה וקריאה של QR Code כתמונה [4] . כל רכב מקודד על פי מס' הרישוי – המזהה הייחודי שלו - קובץ תמונת QRCode שהינה ברשותו.
נקבעה תיקייה מוסכמת משותפת המדמה קרבה פיזית אליה יכתוב רכב "משדר" קובץ תמונה ובהQR Code שלו המכיל את מספר הרישוי שלו. כתיבת הקובץ לתיקייה תסמן קירבה פיזית, מחיקה של הקובץ תסמן ריחוק של הרכבים. אם קובץ זה נמצא בתיקייה אזי מישהו משדר אותו - כלומר נמצא בטווח הזיהוי של חיישני הרכב שלי.

רכבים מנטרים את תיקיית הקרבה בצורה מחזורית ובעת שינוי פותחים את הקבצים מפענחים את התמונה למס' רישוי ויודעים אילו רכבים נמצאים בקרבתם. בכך דימינו חיישן אשר קורא ומפענח מס' המופיע לוחיות הזיהוי של הרכבים שבסביבתו. ומציג את הרכבים אותם הוא רואה ואת סטאטוס התקשורת מולם .

ב. דרישות

בניית 4 ישויות הבאות :

<u>אפליקציה א' : Vehicle</u>

אשר לה מבנה נתונים סטאטי ומשתנה דינאמי בעלת מטודות עיקריות של:

- הקמת ישות מקובץ
- יצירת מפתח פרטי וציבור
- שמירת מפתח ציבורי לקובץ (ללא חתימה)
- קריאת מפתח ציבורי חתום לקובץ
- פתיחת Socket Multicast והאזנה ל Beacons של רכבים אחרים
- שליחת Beacons מחזורי לכתובת Multicast - לצורך החלפת מפתחות
- רכב שולח את הנתונים כולל החתימה של ה CA
- בזמן פתיחת הודעה מאובטחת יוודא חתימה של ה CA
- הגדרה ומימוש פרוטוקול תקשורת להחלפת מפתח
- שמירת מבנה נתונים של רכבים אשר איתם הוקם קשר מפתח ציבורי איתם שליחת הודעה מאובטחת

- פענוח הודעה מאובטחת
- GUI של מידע על הרכב שלי ושל מידע על רכבים שכנים
- אגירת נתונים בפועל של המידע שלי לעומת הנתונים הידועים לרכב
- כתיבת נתונים אחודים לקובץ - עם חתימה מאופסת
- קריאת נתונים מקובץ למבנה הנתונים שלו - עם חתימה אמיתית
- קריאת נתוני QR Code מתיקייה משותפת ודגימתה באופן מחזורי.
- הצגת נתונים שנשלחו והתקבלו וכן סטטוס פענוח ואימות ב - Log ייעודי

<u>אפליקציה ב' : CA</u>

אפליקציה בעלת היכולות הבאות :

- יצירה שמירה וטעינה של מפתחות CA
- קריאה מקובץ של נתוני רכבים לחתימה
- הצגת נתונים על המסך
- חתימת אימות
- שמירת קובץ בעל חתימת אימות

<u>אפליקציה ג' : Attacker</u>

אפליקציה בעלת היכולות הבאות :

- בניית ישות מתקיף – בעל יכולות של רכב – וכולל את ההרחבות הבאות
- מענה לפרוטוקול ל 2 הצדדים והקמת קשר מולם
- פענוח והעברת הודעות בצורה תקינה
- התקפה ושיבוש המידע
- הקלטת הודעות תקשורת
- ניגון מחדש של הודעות מוקלטות
- הצגת נתונים שנשלחו והתקבלו וכן סטטוס פענוח ואימות ב - Log ייעודי

<u>אפליקציה ד' : אפליקציית יצירת QRCode</u>

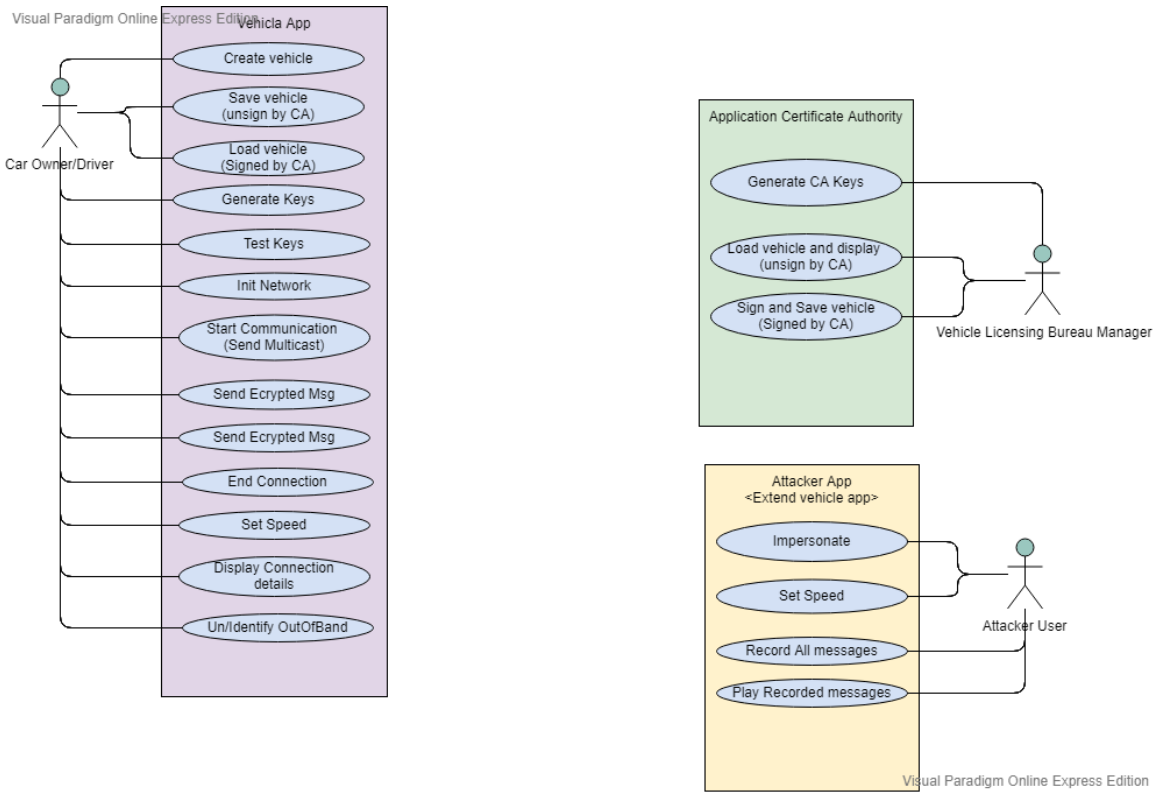
- יצירת קובץ תמונה QRCode מקודד על פי מס' רישוי כקלט
- שמירת QRCode לקובץ תמונה
- טעינה של קובץ QRCode פענוחו והצגת התמונה ומספר הרישוי המפוענח

ג. ממשק משתמש כללי

איור מס' 13 מתאר כיצד נדרש מהאפליקציות להראות באופן סכמטי.

איור מס' 14 מתאר מהן הפעולות הניתנות לביצוע בכל אחת מהאפליקציות.

איור 13 : דרישות ממשקי משתמש



איור 14 : פעילויות אפשריות במערכת ההדגמה

7. כלים ושפת פיתוח לביצוע הפרויקט

הפיתוח פותח עבור מ"ה Windows 10.

שפת פיתוח #C,סביבת פיתוח Visual studio 2017.

כלי עזר נוספים: visual-paradigm,Power Point

8. מימוש הפרויקט

הפרויקט הראשי מחולק למספר תתי פרויקטים

א. הפרויקט Vehicle

המחלקה Vehicle

זוהי המחלקה הראשית של הפרויקט.

המחלקה מייצגת רכב בדרך אשר מתקשר עם העולם (רכבים אחרים) בתקשורת Udp/Ip, תחילה על מנת להקים קשר על ידי שימוש בפרוטוקול החלפת מפתחות , ניתן לבחור את מנגנון האימות רגיל – חתימת CA בלבד או Out Of band חתום CA.

לאחר מכן מאפשר להעביר הודעת מידע מוצפנות– במקרה שלנו אנו מעבירים את מהירותו הנוכחית של הרכב.

כלל המתודות ומבני הנתונים של המחלקה מתוארים באיור מס' 20.

למחלקה המתודות הבאות :

```
InitializeNetwork (string MultycastIpAddress, string MultycastPort, string
LocalIpAddress, string LocalPort)
```

אתחול הרשת, התמנות לכתובת הMulticast על מנת להקשיב להודעות, וכן קישור לכתובת פרטית ופורט מהם שולחים הודעות .

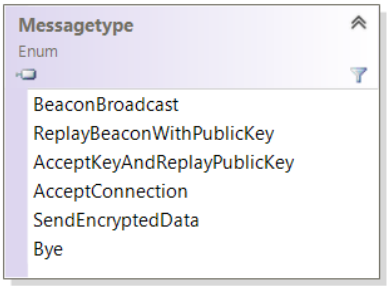
```
InitWorker()
```

אתחול Thread המטפל בשליחה וקבלה של הודעות.

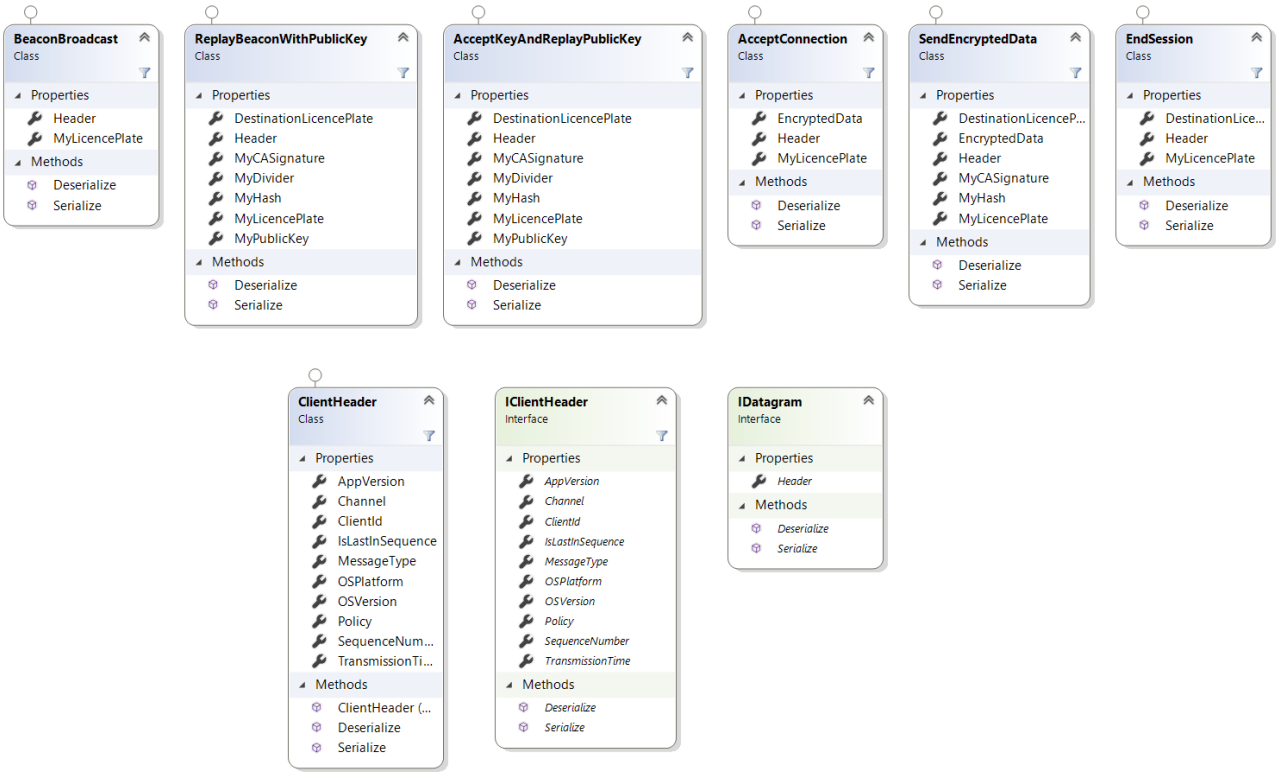
```
ProcessMessage(IDatagram myData)
```

טיפול בהודעה נכנסת אשר מטופל לפי סוג ההודעה . וכן מתודה לכל שליחה של הודעה .

ניתן לראות את סוגי הודעות האפשריות בפרוטוקול איור מס' 15, מבנה הנתונים הנשלח בכל סוג הודעה מתואר באיור מס' 16.

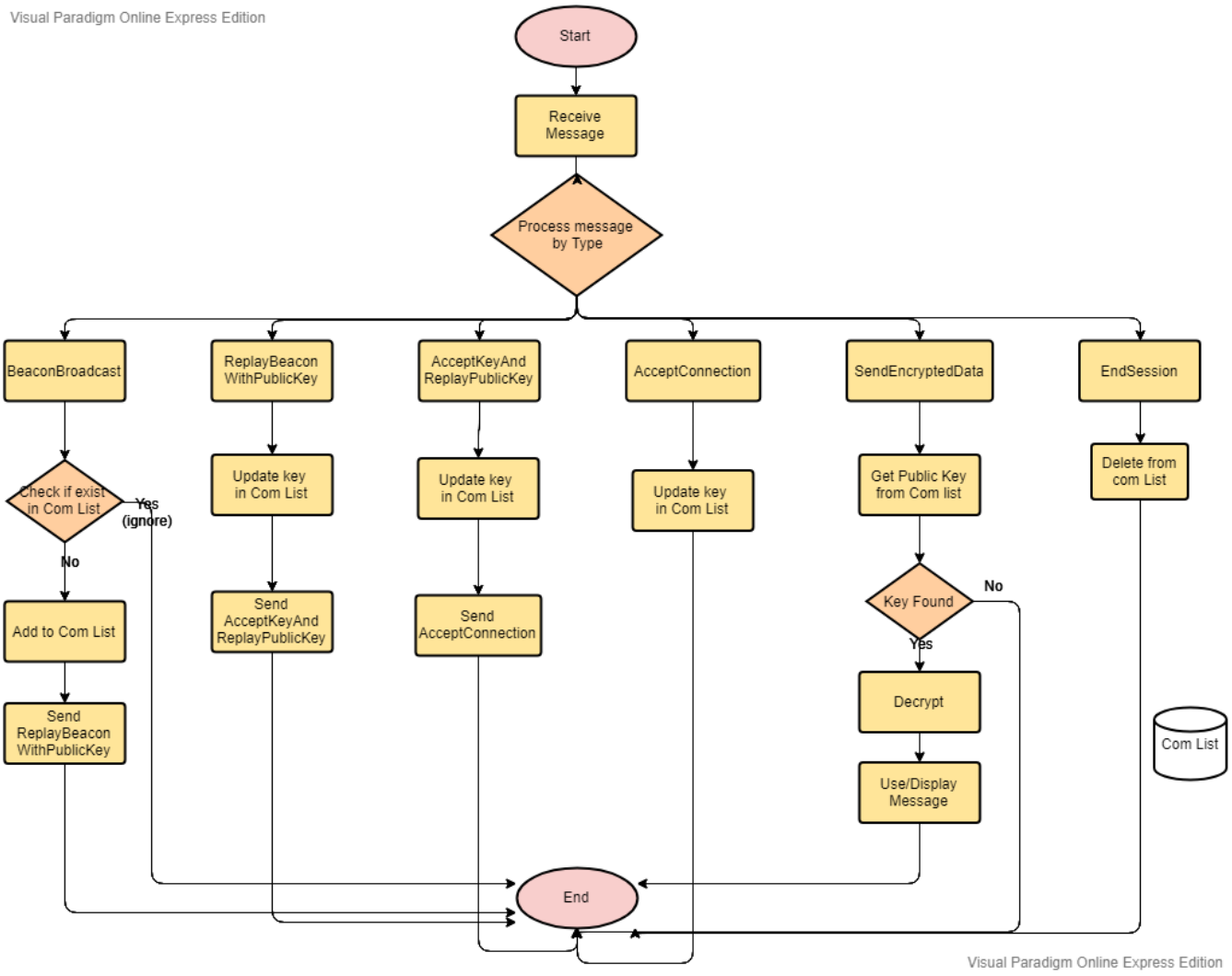


איור 15 : סוגי הודעות אפשריות



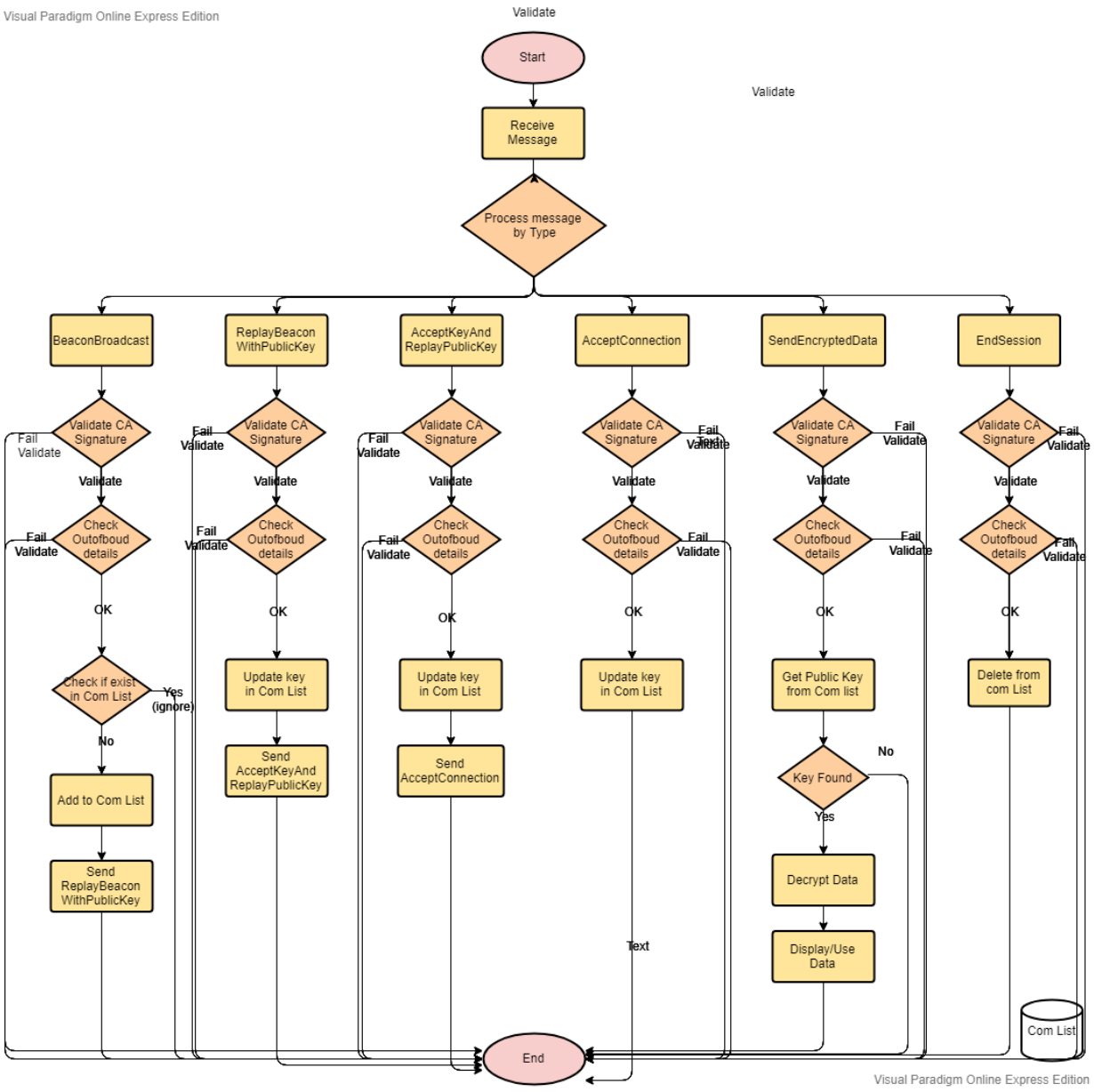
איור 16 : מבנה נתונים של הודעות התקשורת

במוד העבודה ראשון (נאיבי) כאשר מגיעה הודעה לתור ההודעות היא תטופל באופן המודגם באיור מס' 17:



איור 17 : תרשים זרימה (החלפת מפתחות נאיבית)

במוד העבודה השני (מימוש הפרוטוקול המוצע) כאשר מגיעה הודעה לתור ההודעות היא תטופל באופן המודגם באיור מס' 18:



איור 18 : תרשים זרימה החלפת הודעות עם וידוא כפול OutOfBand

```
SendEncryptedData(int licenseNumberToSend)
```

שליחת הודעה מוצפנת ליעד, לאחר הקמת הקשר ותהליך החלפת המפתחות לכל רכב יש את המפתח הציבורי של הרכב הנגדי. המתודה מקבלת קלט : מי נמען ההודעה, מחפשת אותו ברשימת הרכבים במידה ומוצאות אותו וכן סטטוס התקשרות אתו תקין, שולפת את המפתח הציבורי שלו, מצפינה את ההודעה, במקרה שלנו סט פרמטרים הכולל את המהירות הנוכחית של הרכב, ושולחת את ההודעה .

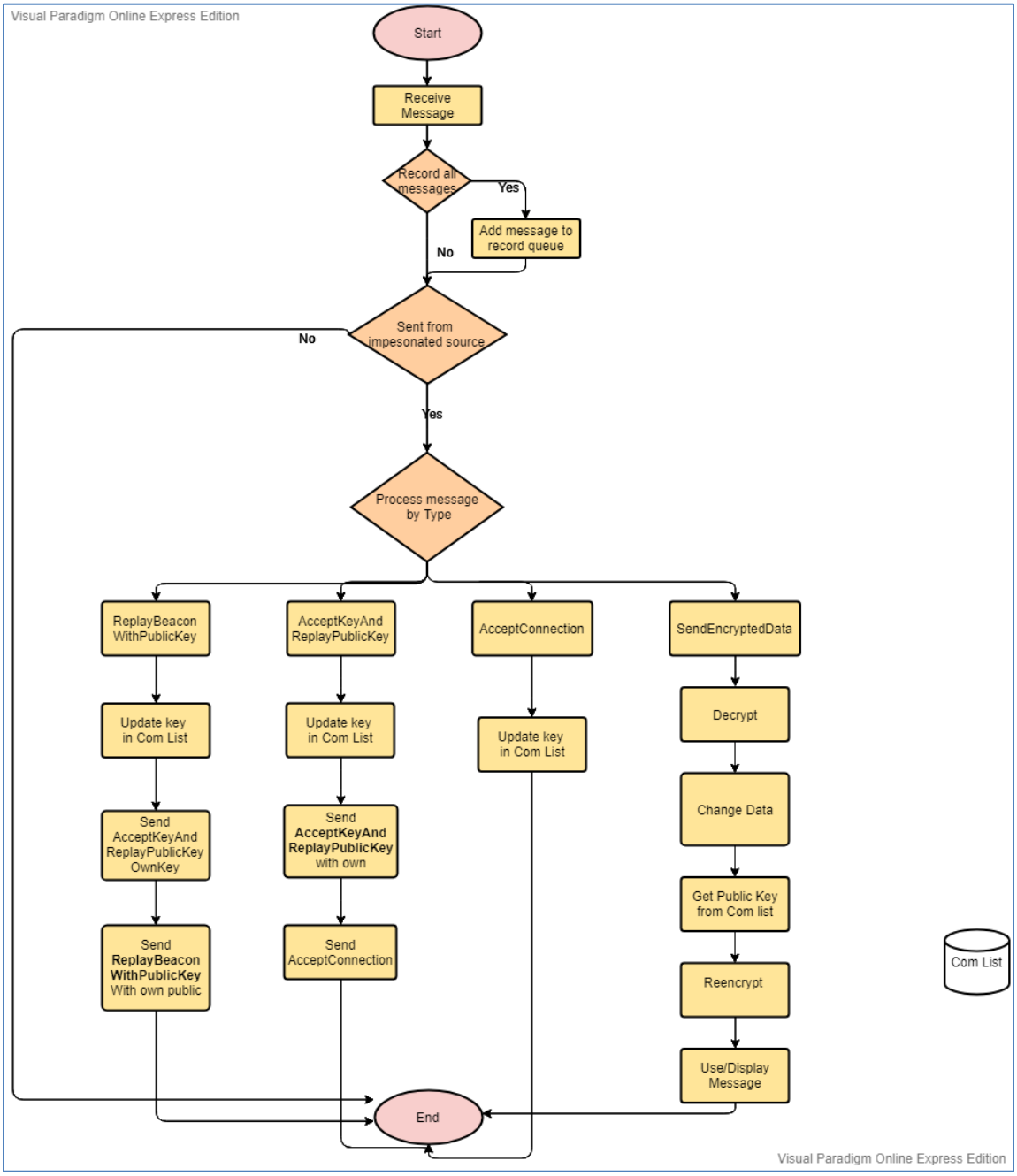
```
Bool ValidateKeyIsSigned(int hash, ulong myCASignature)
```

מתודה זו מקבלת ערבול (Hash) של פרטי רכב וכן חתימה של ה CA על אותו Hash, מתודה זו לוקחת את החתימה, אשר נחתמה באמצעות המפתח הפרטי של ה CA, פותחת אותה באמצעות המפתח הציבורי של ה CA אשר מפורסם באופן חופשי והמידה והנ"ל מתאים לHash זוהי הוכחה כי הפרטים נחתמו על ידי CA והתוצאה הינה True אחרת False.

למחלקת Vehicle ישנה אפשרות להתנהג כתוקף (על ידי אתחול פרמטרי), ובכך יש לה את הכלים להתחזות לכלי רכב אחרים ולהתנהל בשמם, וכן להקליט הודעות ולנגנן במועד מאוחר יותר.

המחלקה Vehicle בתצורת תוקף

אלגוריתם הפעולה של אפליקציית התקיפה מודגם באיור מס' 19:



איור 19 : תרשים זרימה תצורת תוקף (התחזות והקלטה)

```
StartImpersonate(int firstImpersonateId, int seconedImpersonateId)
```

פונקציית תקיפה, התחלת התחזות - המתודה מקבלת כקלט 2 מס' רישוי ייחודים לרכבים, ומעתה האפליקציה תאזין להודעות Multicast ובמידה ומען ההודעות יכילו מספרי רישוי אלו, האפליקציה תתחזה אליהם ותענה במקומם .

```
ReSendEncryptedData(SendEncryptedData sendEncryptedData, UInt64
changedSpeed, int impersonateTo)
```

פונקציית תקיפה, שליחה מחדש של הודעה מוצפנת ליעד , המתודה מקבלת קלט : ההודעה שהתקבלה, הערך החדש שיוזן להודעה וממי התקבלה . במקרה תקיפה כאשר מתחזים לרכב מסוים ומאזינים להודעות אותן הוא שולח, ברשימת התקשרות של התוקף יש מפתחות ציבוריים של הרכבים אליהם התחזה ואילו לרכבים הנתקפים יש את המפתח הציבורי של התוקף (אך הם הוטעו והם חושבים שזהו המפתח הציבורי של הרכב הלגיטימי מולם).

התוקף מיירט את ההודעה מפענח אותה באמצעות המפתח הפרטי שלו, משנה את תוכנה של ההודעה במקרה שלנו מהירות הרכב, מצפין אותה מחדש באמצעות המפתח הציבורי של הרכב הנגדי ושולח אותה

```
StartRecord(), StopRecord()
```

פונקציית תקיפה, התחלת וסיום הקלטת הודעות
כל ההודעות הנקלטות לכתובת ה Multicast נשמרות ללא שינוי בתור הודעות ייעודי.

```
StartPlay()
```

פונקציית תקיפה, ניגון הקלטה - כל ההודעות שנשמרו בתור ההודעות הייעודי מנוגנות על פי סדר הקלטתם מחדש לכתובת ה Multicast .

ב. הפרויקט General

מחלקה EncryptionHelper

מחלקה זו מכילה מתודות סטאטיות אשר מאפשרות סט יכולות הצפנה בסיסיות

```
bool GeneratePrivatePublicKeys(UInt64 maxPrime, out UInt64 PublicKey,out
UInt64 PrivateKey, out UInt64 divider)
```

מתודה זו מייצרת מפתח פרטי ומפתח ציבורי וכן divider הנדרש להצפנה ופענוח פיתוח המתודות על פי RSA [5] .
המחלקה Vehicle משתמשת במתודה על מנת לייצר מפתחות הצפנה לרכב.
המחלקה Certification Authority משתמשת במתודה על מנת לייצר מפתחות הצפנה לCA על מנת לחתום על פרטי רכב.

```
UInt64 GeneratePrimeNumber(UInt64 maxPrime)
```

יצירת מספר ראשוני, מתודת יצירת מפתחות זקוקה לשני מספרים ראשוניים, המתודה מגרילה מספר גדול ומנסה לבדוק האם הוא ראשוני, אם כן מחזירה אותו, אם לא מגרילה מס' נוסף ונסה עד להצלחה.

```
EncryptMessage(UInt64 msg, UInt64 publicKey, UInt64 divider)
```

הצפנת הודעה באמצעות מפתח ציבורי

```
DecryptMessage(UInt64 msg, UInt64 privateKey, UInt64 divider)
```

פענוח הודעה באמצעות מפתח פרטי

```
SignMessage(UInt64 msg, UInt64 privateKey, UInt64 divider)
```

חתימה על הודעה באמצעות מפתח פרטי, ההודעה עוברת תהליך ערבול (Hash) ועליו מתבצעת החתימה בפועל.

```
VerifySignatureMessage(UInt64 signature, UInt64 msg, UInt64 publicKey,
UInt64 divider)
```

בדיקת אימות חתימה על הודעה באמצעות מפתח ציבורי, בדיקת האימות הינה על חתימה על הודעה לאחר שעברה תהליך ערבול (Hash) .

```
int CalcHashOnASCIIArray(byte[] arr)
```

מתודת ערבול מערך bytes למספר אחד (הנחה לצורך פשטות – על פני חד ערכיות) , לטובת קלות בחתימה ובאימות על מספר אחד מאשר על הודעה ארוכה.

```
CalculatePublicKey(UInt64 euler)
```

חישוב מפתח ציבורי על פי קלט מספר אוילר

```
CalculatePrivateKey(UInt64 a, UInt64 b)
```

חישוב מפתח פרטי

מחלקה GenericUtils

מחלקת עזר לשמירת פרטי אובייקט בקובץ xml.

```
bool Save<T>(string FileName, Object Obj)
```

שמירת אובייקט (בד"כ משתמשים באובייקט מסוג Vehicle) ושמירתו כקובץ נתונים, משמש להעברת נתונים בין Vehicle app ל CA app – לצורך וידוא וחתימה, וכן לטעינה מהירה של רכב קיים.

```
T Load<T>(string FileName)
```

טעינת אובייקט (בד"כ משתמשים באובייקט מסוג Vehicle) ושמירתו כקובץ נתונים, משמש להעברת נתונים בין Vehicle app ל CA app – לצורך וידוא וחתימה, וכן לטעינה מהירה של רכב קיים.

ג. הפרויקט Certification Authority

מחלקה CertificateAuthorityForm

מחלקה בבסיס האפליקציה של ה Certification Authority

```
GenerateKeys()
```

מתודה ליצירה פסאודו רנדומלית של מפתחות Certification Authority
מתודה מייצרת מפתח פרטי וציבורי.
את המפתח הציבורי יש להפיץ לכלל המשתמשים אתו יוכלו לאמת חתימות .

```
LoadVehicleFromFile(String fileName)
```

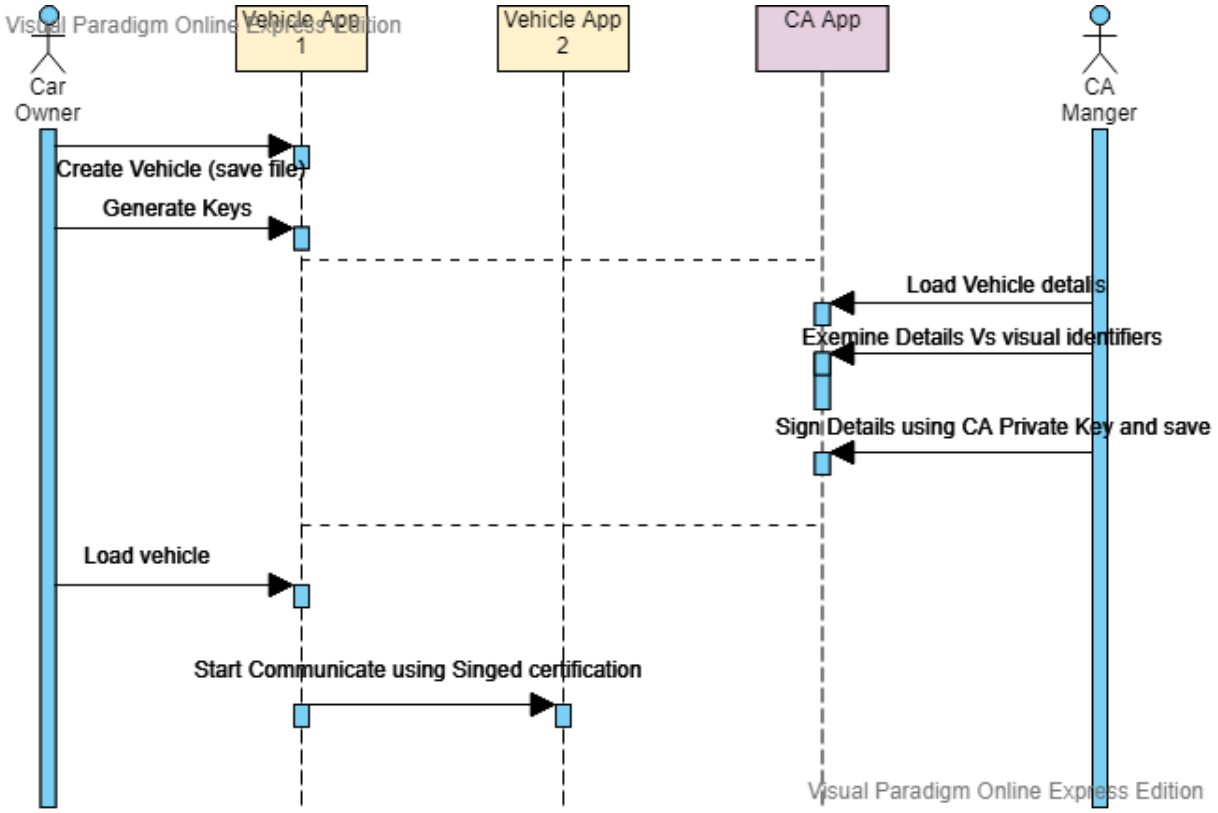
מתודה לשליפת נתוני רכב מקובץ - לאחר שנשמר על ידי אפליקציית vehicle.
לצורך הצגתם על המסך ובחינתם על ידי משתמש מוסמך לאשר אותם.

```
SignCert()
```

מתודה אשר יוצרת מפרטי הרכב Hash ובאמצעות המפתח הפרטי שלה חותמת אותו,
את החתימה מוסיפה לנתוני האובייקט .

```
SaveVehicleToFile(String fileName)
```

מתודה לשמירת נותני רכב לקובץ, נשמר כולל נתוני החתימה החדשים לצורך שליפתם
באפליקציית Vehicle ושימוש בחתימה וצורך זיהוי.
איור מס' 21 ממחיש את האינטראקציה בין האפליקציות לצורך חתימה.



איור 21 : חתימת CA על פרטי רכב

ד. הפרויקט QRCodeCraetor

מחלקה QRCodeCreatorForm

```
CreateQRCode()
```

יצירת ברקוד QR המקודד את מס' הרישוי של הרכב .
לצורך כך נעשה שימוש בספריית קוד פתוח [6]
MessagingToolkit.QRCode.Codec.QRCodeEncoder

```
SaveQRToFile()
```

מתודה לשמירת ברקוד QR כקובץ תמונה במערכת הקבצים.
הנ"ל שימושי לצורך שליפה מהירה ללא יצירה וכן הקובץ משמש להעתקה לתיקיית קרבה לצורך זיהוי פיזי Out of Band.

```
LoadQRFromFile()
```

מתודה לשליפת קובץ תמונה ממערכת הקבצים פענוחו כברקוד QR למספר רישוי.

מחלקה Watcher

```
OnChanged(object source, FileSystemEventArgs e)
```

מתודה הנרשמת לאירועי שינוי במערכת הקבצים בתיקיית הקרבה הפיזית ומופעלת אימת שיש שינוי, בהפעלתה תקרא את כל קבצי הברקוד הנמצאים בתיקייה תפענח אותם ותציג על המסך כמו כן תשמור ברשימה על מנת לבחון בעת תשאול האם רכב בעל מספר רישוי כלשהו נמצא בקרבתנו .

9. תוצאות

א. הקמת ערוץ תקשורת חתום על ידי CA תסריט תקין

תקשורת מוצפנת (נאיבית) בין 2 רכבים : הקמת קשר, החלפת מפתחות ושליחת הודעות מוצפנות.

<u>לוג הודעות של רכב א – רישוי 5555</u>

יוזם הודעת משואה, מקבל מפתח ציבורי של 1111, שולח מפתח ציבורי של עצמו.
שולח 2 הודעות מוצפנות עם המהירות הנוכחית שלו 45 ולאחר מכן 73 .

```
09.54.35.78 : Load Save Vehicle To File, File name :C:\Temp\t2Signed.xml
09.54.39.55 : Send broadcast beacon
09.54.39.60 : Receive ReplayBeaconWithPublicKey message from Vehicle : 1111
09.54.39.61 : Vehicle : 1111 ReplayBeaconWithPublicKey validate successfully - processing message
09.54.39.61 : Vehicle : 1111 new connection adding into list
09.54.39.62 : Send Replay With Own Public Key Messages
09.54.39.67 : Receive Accept connection message from Vehicle : 1111
09.54.39.68 : Vehicle : 1111  Already in com list processing message
09.54.39.69 : secure connection with : 1111 Established
09.54.48.34 : Vehicle : 1111  Already in comList try to send message
09.54.48.34 : Encrypt Data Current speed : 45
09.54.48.35 : Message encrypted, Sending message
09.54.48.35 : Send Encrypted Data message id : 1
09.54.51.36 : Vehicle : 1111  Already in comList try to send message
09.54.51.37 : Encrypt Data Current speed : 73
09.54.51.37 : Message encrypted, Sending message
09.54.51.37 : Send Encrypted Data message id : 2
```

<u>לוג הודעות של רכב ב – רישוי 1111</u>

מקבל הודעת משואה, שולח מפתח ציבורי שלו, מקבל מפתח ציבורי של 5555 שולח קשר הוקם. מקבל 2 הודעות של מהירות רכב 5555 אחת של 45 ולאחר מכן 73.

```
09.54.36.41 : Load Save Vehicle To File, File name :C:\Temp\t1Signed.xml
09.54.39.57 : Receive Beacon message from Vehicle : 5555
09.54.39.58 : Vehicle : 5555 new connection adding into list
09.54.39.59 : Send Replay With Own Public Key Messages
09.54.39.63 : Receive Accepted Key message from Vehicle : 5555
09.54.39.64 : Vehicle : 5555 Accepted Key validate successfully - processing message
09.54.39.65 : Vehicle : 5555  Already in com list dropping Existing Key message
09.54.39.66 : Vehicle : 5555 new connection adding into list
09.54.39.67 : Send Accept Connection
09.54.39.68 : Send Accept connection to vehicle : 5555
09.54.39.69 : secure connection with : 5555 Established
09.54.48.35 : Receive Encrypted data message from Vehicle : 5555
09.54.48.36 : Vehicle : 5555  Already in comList processing message
09.54.48.36 : Message decrypted, Vehicle : 5555 speed is : 45
09.54.51.37 : Receive Encrypted data message from Vehicle : 5555
09.54.51.38 : Vehicle : 5555  Already in comList processing message
09.54.51.38 : Message decrypted, Vehicle : 5555 speed is : 73
```

ב. הקמת ערוץ תקשורת חתום על ידי CA תסריט התקפת MitM

<u>לוג הודעות של רכב א – רישוי 5555</u>

זהה להדגמה הנאיבית – ההודעות המוצפנות הינן בערך 41 ו 73 .

```
09.15.03.85 : Load Save Vehicle To File, File name :C:\Temp\t2Signed.xml
09.15.30.19 : Send broadcast beacon
09.15.30.22 : Receive ReplayBeaconWithPublicKey message from Vehicle : 1111
09.15.30.23 : Vehicle : 1111 ReplayBeaconWithPublicKey validate successfully - processing
message
09.15.30.24 : Vehicle : 1111 new connection adding into list
09.15.30.24 : Send Replay With Own Public Key Messages
09.15.30.26 : Receive Accept connection message from Vehicle : 1111
09.15.30.27 : Vehicle : 1111  Already in com list processing message
09.15.30.27 : secure connection with : 1111 Established
09.15.30.77 : Receive Accept connection message from Vehicle : 1111
09.15.30.78 : Vehicle : 1111  Already in com list processing message
09.15.30.79 : secure connection with : 1111 Established
09.15.31.26 : Receive ReplayBeaconWithPublicKey message from Vehicle : 1111
09.15.31.27 : Vehicle : 1111 ReplayBeaconWithPublicKey validate successfully - processing
message
09.15.31.28 : Vehicle : 1111 is in comlist processing message ...
09.15.31.29 : Vehicle : 1111 new connection adding into list
09.15.31.30 : Send Replay With Own Public Key Messages
09.15.35.20 : Vehicle : 1111  Already in com list processing message
09.15.35.21 : secure connection with : 1111 Established
09.15.35.21 : Receive Accept connection message from Vehicle : 1111
09.15.35.22 : Vehicle : 1111  Already in com list processing message
09.15.35.23 : secure connection with : 1111 Established
09.15.51.14 : Vehicle : 1111  Already in comList try to send message
09.15.51.14 : Encrypt Data Current speed : 41
09.15.51.14 : Message encrypted, Sending message
09.15.51.15 : Send Encrypted Data message id : 1
09.16.18.31 : Vehicle : 1111  Already in comList try to send message
09.16.18.32 : Encrypt Data Current speed : 73
09.16.18.32 : Message encrypted, Sending message
09.16.18.32 : Send Encrypted Data message id : 2
```

לוג הודעות של תוקף – רישוי 9999

תחילה מזדהה כשני הרכבים (1111,5555) עונה בשמם בשלב הקמת הקשר
ומחליף מפתחות, בעת קבלת הודעה מוצפנת משנה את ערכה ושולח אותה מחדש

```
09.14.56.62 : Load Save Vehicle To File, File name :C:\Temp\attackerSigned.xml
09.15.24.82 : ImpersonateMode Start, FirstImpersonateId : 1111 SeconedImpersonateId : 5555
09.15.30.22 : Receive ReplayBeaconWithPublicKey message from Vehicle : 1111
09.15.30.24 : Vehicle : 1111 ReplayBeaconWithPublicKey validate successfully - processing
message
09.15.30.25 : Vehicle : 1111 new connection adding into list
09.15.30.75 : Send Replay With Impersonate Id Messages : 5555
09.15.31.26 : Send Replace  ReplayBeaconWithOwnPublicKeyMessages With Impersonate Id
Messages : 1111
09.15.31.28 : Receive Accepted Key message from Vehicle : 5555
09.15.31.29 : Vehicle : 5555 Accepted Key validate successfully - processing message
09.15.31.81 : Send Accept Connection
09.15.31.82 : Send Accept connection With Impersonate Id Messages : 1111 to vehicle : 5555
09.15.32.34 : Send Replay With Impersonate Id Messages : 5555
09.15.32.35 : secure connection with : 5555 Established
09.15.32.35 : Receive Accept connection message from Vehicle : 1111
09.15.32.36 : Vehicle : 1111  Already in com list processing message
09.15.32.36 : secure connection with : 1111 Established
09.15.32.39 : Receive Accepted Key message from Vehicle : 5555
09.15.32.39 : Vehicle : 5555 Accepted Key validate successfully - processing message
09.15.32.40 : Vehicle : 5555  Already in com list droping Existing Key message
09.15.32.40 : Vehicle : 5555 new connection adding into list
09.15.32.90 : Send Accept Connection
09.15.32.92 : Send Accept connection With Impersonate Id Messages : 1111 to vehicle : 5555
09.15.33.43 : Send Replay With Impersonate Id Messages : 5555
09.15.33.43 : secure connection with : 5555 Established
09.15.33.44 : Receive Accept connection message from Vehicle : 1111
09.15.33.45 : Vehicle : 1111  Already in com list processing message
09.15.33.47 : secure connection with : 1111 Established
09.15.33.47 : Receive Accept connection message from Vehicle : 1111
09.15.33.47 : Vehicle : 1111  Already in com list processing message
09.15.33.48 : secure connection with : 1111 Established
09.15.51.15 : Receive Encrypted data message from Vehicle : 5555
09.15.55.20 : Vehicle : 5555  Already in comList processing message
09.15.55.21 : Message decrypted, Vehicle : 5555 speed is : 41
09.15.55.22 : Message encrypted, Sending message
09.15.55.22 : Send Encrypted Data
09.15.55.23 : ReSend Rencrypted Data to  : 5555
09.16.18.32 : Receive Encrypted data message from Vehicle : 5555
09.16.18.33 : Vehicle : 5555  Already in comList processing message
09.16.18.33 : Message decrypted, Vehicle : 5555 speed is : 73
09.16.18.34 : Message encrypted, Sending message
09.16.18.34 : Send Encrypted Data
09.16.18.35 : ReSend Rencrypted Data to  : 5555
```

לוג הודעות של רכב ב – רישוי 1111

זהה להדגמה הנאיבית. ניתן לראות כי מקבל 4 הודעות מוצפנות – 2 מקוריות אותן אינו מצליח לפענח ומקבל ערך לא חוקי – אלו ההודעות המקוריות של רכב 5555 אך אין ברשות 1111 את המפתח .
2 הודעות נוספות אותן הוא מקבל הינן "מטופלות" וערכן שונה (התוקף הוסיף 40 לערך המקורי) והן 81 ו 113 .

```
09.15.04.78 : Load Save Vehicle To File, File name :C:\Temp\t1Signed.xml
09.15.30.20 : Receive Beacon message from Vehicle : 5555
09.15.30.21 : Vehicle : 5555 new connection adding into list
09.15.30.22 : Send Replay With Own Public Key Messages
09.15.30.25 : Receive Accepted Key message from Vehicle : 5555
09.15.30.25 : Vehicle : 5555 Accepted Key validate successfully - processing message
09.15.30.25 : Vehicle : 5555  Already in com list droping Existing Key message
09.15.30.26 : Vehicle : 5555 new connection adding into list
09.15.30.26 : Send Accept Connection
09.15.30.27 : Send Accept connection to vehicle : 5555
09.15.30.27 : secure connection with : 5555 Established
09.15.30.75 : Receive Accepted Key message from Vehicle : 5555
09.15.30.76 : Vehicle : 5555 Accepted Key validate successfully - processing message
09.15.30.76 : Vehicle : 5555  Already in com list droping Existing Key message
09.15.30.76 : Vehicle : 5555 new connection adding into list
09.15.30.77 : Send Accept Connection
09.15.32.37 : Send Accept connection to vehicle : 5555
09.15.32.38 : secure connection with : 5555 Established
09.15.33.43 : Receive Accepted Key message from Vehicle : 5555
09.15.33.43 : Vehicle : 5555 Accepted Key validate successfully - processing message
09.15.33.44 : Vehicle : 5555  Already in com list droping Existing Key message
09.15.33.45 : Vehicle : 5555 new connection adding into list
09.15.33.47 : Send Accept Connection
09.15.33.47 : Send Accept connection to vehicle : 5555
09.15.33.47 : secure connection with : 5555 Established
09.15.51.15 : Receive Encrypted data message from Vehicle : 5555
09.15.51.16 : Vehicle : 5555  Already in comList processing message
09.15.51.16 : Message decrypted, Vehicle : 5555 speed is : 89463595
09.15.55.22 : Receive Encrypted data message from Vehicle : 5555
09.15.55.23 : Vehicle : 5555  Already in comList processing message
09.15.55.24 : Message decrypted, Vehicle : 5555 speed is : 81
09.16.18.32 : Receive Encrypted data message from Vehicle : 5555
09.16.18.33 : Vehicle : 5555  Already in comList processing message
09.16.18.33 : Message decrypted, Vehicle : 5555 speed is : 207663269
09.16.18.34 : Receive Encrypted data message from Vehicle : 5555
09.16.18.34 : Vehicle : 5555  Already in comList processing message
09.16.18.35 : Message decrypted, Vehicle : 5555 speed is : 113
```

ג. הקמת ערוץ תקשורת חתום על ידי CA כולל אימות Out of band תסריט התקפת ניגון מחדש של הודעות עבר

<u>לוג הודעות של רכב א – רישוי 1111</u>

הפרוטוקול דומה לפרוטוקול של החלפת המפתחות הקודם, אך בשינוי אחד – בעת אימות כי ההודעה נחתמה על ידי CA, גם התוכן החתום נבחן ואת מס' הרישוי בהודעה מנסים לאמת על ידי חיישן (במקרה שלנו קריאת QRCode מתיקיית הקרבה) ורק אם מס' הרישוי החתום נמצא בסביבה בעת האימות מדפסים את ההודעה "validate out of band successfully" וממשיכים בפרוטוקול החלפת המפתחות. על פי הלוג רכב 1111 מחליף מפתחות עם אימות Out of band עם רכב 5555 , לאחר החלפת המפתחות שולח 2 הודעות מוצפנות עם המהירות הנוכחית שלו

```
08.21.46.34 : Load Save Vehicle To File, File name :C:\Temp\t1Signed.xml
08.22.38.19 : Send broadcast beacon
08.22.38.22 : Receive ReplayBeaconWithPublicKey message from Vehicle : 5555
08.22.38.23 : Vehicle : 5555 ReplayBeaconWithPublicKey validate successfully - processing message
08.22.38.23 : Vehicle : 5555 ReplayBeaconWithPublicKey validate out of band successfully - processing message
08.22.38.24 : Vehicle : 5555 new connection adding into list
08.22.38.25 : Send Replay With Own Public Key Messages
08.22.38.28 : Receive Accept connection message from Vehicle : 5555
08.22.38.29 : Vehicle : 5555  Already in com list processing message
08.22.38.30 : secure connection with : 5555 Established
08.23.08.37 : Vehicle : 5555  Already in comList try to send message
08.23.08.38 : Encrypt Data Current speed : 33
08.23.08.38 : Message encrypted, Sending message
08.23.08.38 : Send Encrypted Data message id : 1
08.23.11.54 : Vehicle : 5555  Already in comList try to send message
08.23.11.54 : Encrypt Data Current speed : 69
08.23.11.55 : Message encrypted, Sending message
08.23.11.55 : Send Encrypted Data message id : 2
```

<u>לוג הודעות של רכב תוקף – רישוי .</u>

N/A מבצע הקלטה של 2 ההודעות המוצפנות מבלי לדעת את תוכנן פעמיים - פעם אחת כאשר הרכב המוקלט בסביבה וניתן לבצע אימות Out of band מולו. פעם שניה כאשר הוא איננו ולא ניתן לאמת .

```
08.22.50.81 : Load Save Vehicle To File, File name :C:\Temp\attackerSigned.xml
08.23.08.39 : record message type : SendEncryptedDataRecord counter 1
08.23.11.55 : record message type : SendEncryptedDataRecord counter 2
08.23.29.73 : Send recorded message type : SendEncryptedDataRecord counter 1
08.23.29.84 : Send recorded message type : SendEncryptedDataRecord counter 2
08.24.27.67 : Send recorded message type : SendEncryptedDataRecord counter 1
08.24.27.78 : Send recorded message type : SendEncryptedDataRecord counter 2
```

<u>לוג הודעות של רכב ב – רישוי 5555</u>

מחליף מפתחות עם אימות Out of band עם רכב 1111 , לאחר החלפת המפתחות מקבל 2 הודעות מוצפנות מרכב 5555 מבצע אימות Out of band ומפענחן .

לאחר מכן מקבל 2 הודעות מוצפנות נוספות – התוקף שולח הודעות ישנות, הוא מבצע אימות מול 5555 שעדיין בסביבה ומפענחן.

לאחר מכן מקבל 2 הודעות מוצפנות נוספות – התוקף שולח הודעות ישנות, הוא מנסה לבצע אימות מול 5555 שכבר אינו בסביבה ונכשל לאמתן – זורק את ההודעות

```
08.21.47.60 : Load Save Vehicle To File, File name :C:\Temp\t2Signed.xml
08.22.38.20 : Receive Beacon message from Vehicle : 1111
08.22.38.21 : Vehicle : 1111 new connection adding into list
08.22.38.22 : Send Replay With Own Public Key Messages
08.22.38.25 : Receive Accepted Key message from Vehicle : 1111
08.22.38.26 : Vehicle : 1111 Accepted Key validate successfully - processing message
08.22.38.26 : Vehicle : 1111  Accepted Key validate out of band successfully - processing message
08.22.38.27 : Vehicle : 1111  Already in com list dropping Existing Key message
08.22.38.27 : Vehicle : 1111 new connection adding into list
08.22.38.28 : Send Accept Connection
08.22.38.29 : Send Accept connection to vehicle : 1111
08.22.38.30 : secure connection with : 1111 Established
08.23.08.39 : Receive Encrypted data message from Vehicle : 1111
08.23.08.39 : Vehicle : 1111  Already in comList processing message
08.23.08.40 : Message decrypted, Vehicle : 1111 speed is : 33
08.23.11.55 : Receive Encrypted data message from Vehicle : 1111
08.23.11.56 : Vehicle : 1111  Already in comList processing message
08.23.11.57 : Message decrypted, Vehicle : 1111 speed is : 69
08.23.29.73 : Receive Encrypted data message from Vehicle : 1111
08.23.29.74 : Vehicle : 1111  Already in comList processing message
08.23.29.74 : Message decrypted, Vehicle : 1111 speed is : 33
08.23.29.84 : Receive Encrypted data message from Vehicle : 1111
08.23.29.85 : Vehicle : 1111  Already in comList processing message
08.23.29.86 : Message decrypted, Vehicle : 1111 speed is : 69
08.24.27.66 : Receive Encrypted data message from Vehicle : 1111
08.24.27.67 : Vehicle : 1111  Accepted Key fail to validate out of band - dropping message
08.24.27.77 : Receive Encrypted data message from Vehicle : 1111
08.24.27.78 : Vehicle : 1111  Accepted Key fail to validate out of band - dropping message
```

10. מסקנות / סיכום

תקשורת בין רכבים בדרך מטבעה הינה אלחוטית ועקב כך חשופה לתקיפות רשת והאזנות והפרת פרטיות חברי הקבוצה. תקיפות דרך רשת התקשורת עשויות לתת לתוקף פוטנציאלי רווח בהשגת יתרון בדרך, השגת מידע פרטי על נהגים/מכוניות, וגרימת נזק כחלק מאירוע פלילי או טרוריסטי. מכיוון שחלק משמעותי מרשת תקשורת בין רכבית הינה שליטה בזמן אמת על כלי רכב ועל תנועתם במרכב בדרך כלל במהירויות גבוהות, משמעות התקפה עליהן עלולה להוביל לתאונות דרכים ואף לעלות בחיי אדם.

יש צורך לתת מענה בדמות פתרונות אבטחה מסוגים שונים לסוגי התקפות שונות במקרה של פרויקט זה ניתן דגש על סוג מסוים של התקפה והיא תודגם בו במספר שלבי אבולוציה ובמיוחד בנושא האימות הכפול של ה CA על נתוני Out of Band .

מימוש האלגוריתם יעזור לעמוד על המורכבות, הקשיים, והיעילות של השימוש בשיטת : *Vehicle authentication via monolithically certified public key and attributes*.

המאמר מספק דרך להתמודד עם התקפת האדם שבתווך על ידי שימוש חתימה מראש על נתונים על הרכב ואימותם בזמן אמת בדרך Out of band. הוצג האלגוריתם וכן הצעה למבנה תעודה דיגיטלית חתומה על ידי רשות מאושרת, וכן הוצגו שיטות להתקפת השיטה על ידי הקלטת התקשורת וניגונה מחדש ושיפורים/שינויים שניתן להוסיף לאלגוריתם על מנת להתמודד מאידך.

נראה כי גם במקרה של התחזות, ניתן לגלות אותה שכן אם מתחזים לרכב לגיטימי עדיין נשלחת ההודעה של הרכב הלגיטימי באוויר ולאחריה נשלחת הודעה מתחזה ומשונה . ללא יכולות לגרום להודעה להיעלם/להתקלקל בדרך, אזי הרכבים יקבלו הודעות כפולות/משונות.

על אף כי הפרוטוקול שלהם מאפשר שליחה מחדש ומענה על הודעות, לדעתי מערכת IDS (Intrusion Detection System) יכולה לסייע במציאת אנומליות והתנהגות לא אופיינית במקרה של תקיפה.

נראה כי Validation רגיל ללא OutOfBand details יכול למנוע מצב של התחזות בשעת החלפת מפתחות, שכן לא ניתן להתחזות לרכב אחר עם מפתח שונה ועדיין להיות חתום על ידי CA. הנ"ל מאפשר התמודדות עם הקלטת הודעות וניגונן מחדש בשלב מאוחר יותר שכן מחייב אימות עם פרמטרים סטטיים של הרכב הנתינים לזיהוי כאשר הוא מתקרב באמצעות סנסורים. נדמה כי הנ"ל אינו נותן מענה מלא שכן גם פרמטרים סטטיים אלו ניתן במאמץ לזייף .

הערה : בתחילה התכוונתי לקיים השהיה קבועה בעת העברת הודעה רגילה על מנת לתת אפשרות לתוקף לשלוח הודעה אשר תתקבל בזמן .
במהלך העבודה התברר כי הנ"ל אינו ניתן לביצוע שכן לא ניתן לבצע השהיה בתווך האוויר ויהיה לא נכון לקיים זאת . המפתח להתקפה הינו היכולת להחליף מפתח לאחר שכבר נקבע כחלק מהפרוטוקול , במידה ומנטרלים יכולת זו – האפשרות להתקפה פוחתת משמעותית .

11. רשימת מקורות

[1] Shlomi Dolev, Łukasz Krzywiecki, Nisha Panwar, Michael Segal. Vehicle authentication via monolithically certified public key and attributes
Wireless Networks 22(3): 879-896 (2016)

[2] Mario Gerla, Joshua Joy (2017(. Internet of Vehicles and Autonomous Connected Car - Privacy and Security Issues. Proceedings of 26th International Conference on Computer Communication and Networks (ICCCN), 2017

[3] A. Kesting, M. Treiber, and D. Helbing, (2010) “Enhanced intelligent driver model to access the impact of driving strategies on traffic capacity.”
Philosophical transactions. Series A, Mathematical, physical, and engineering sciences, vol. 368, no. 1928, pp. 4585–605,.

[4] McCune, J.M., Perrig, A., & Reiter, M.K. (2005). Seeing-isbelieving: “Using camera phones for human-verifiable authentication”.In proceedings of IEEE Symposium on Security and Privacy (pp.110–124), 2005

[5] www.Wikipedia.org

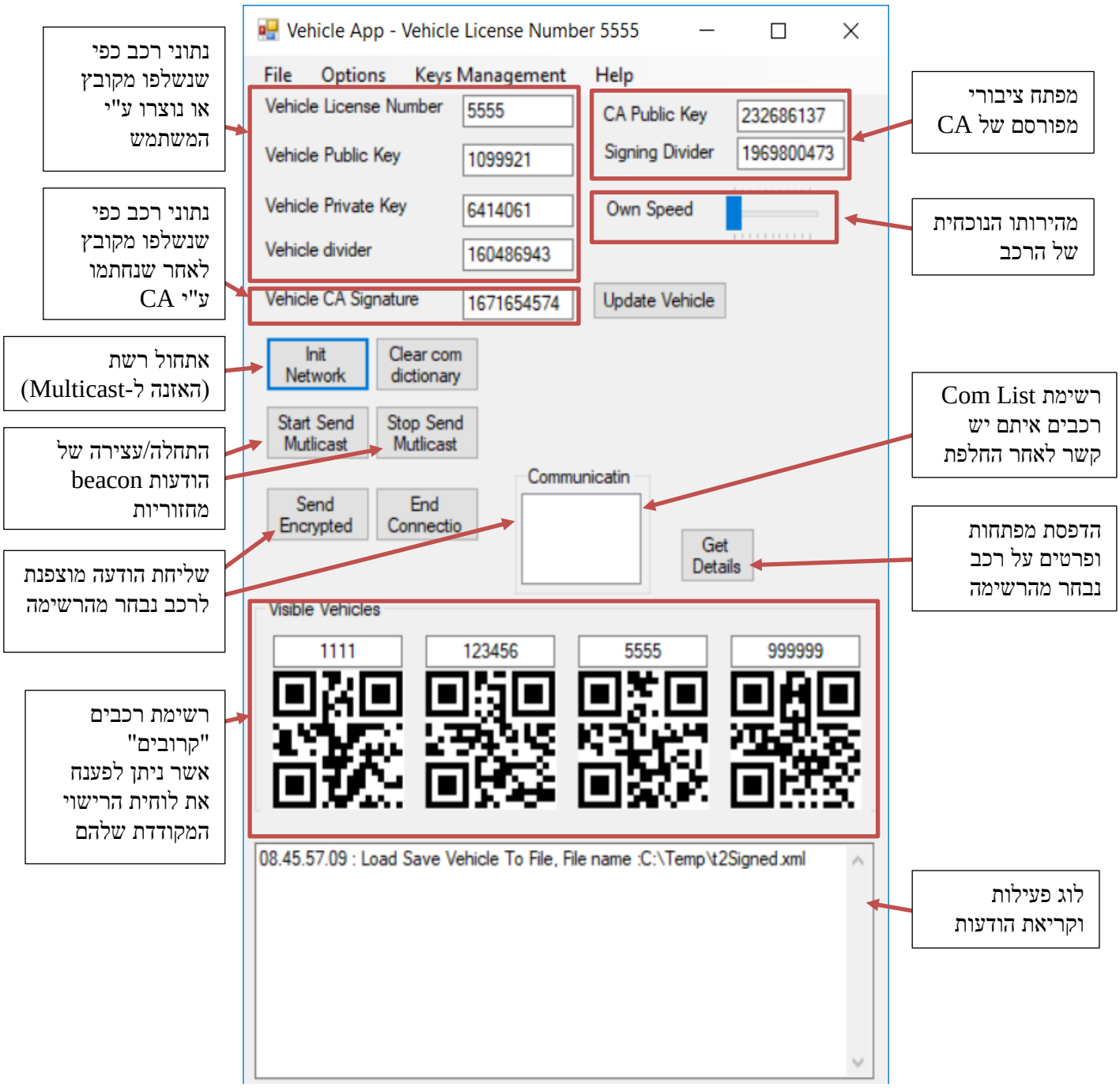
[6] https://www.nuget.org/packages/MessagingToolkit.QRCode

12. נספחים

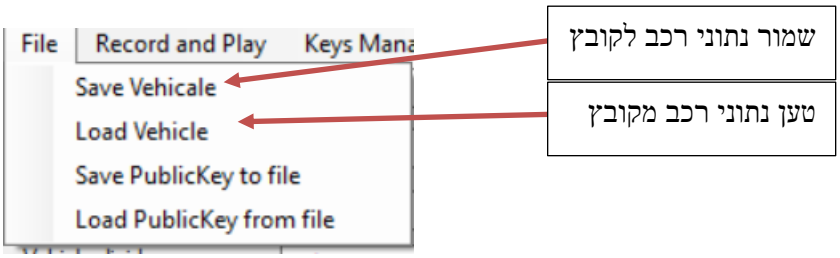
א. מסכי אפליקציות ומדריך שימוש

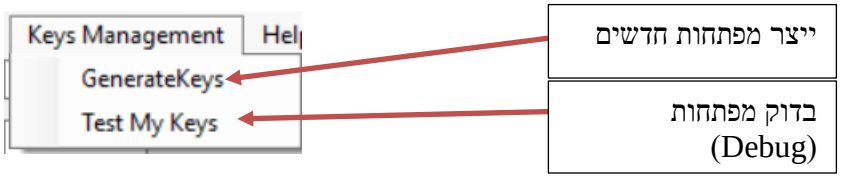
מסכי אפליקציית Vehicle

ראה איורים מס' 22 ו 23.



איור 22 : ממשק משתמש אפליקציית Vehicle

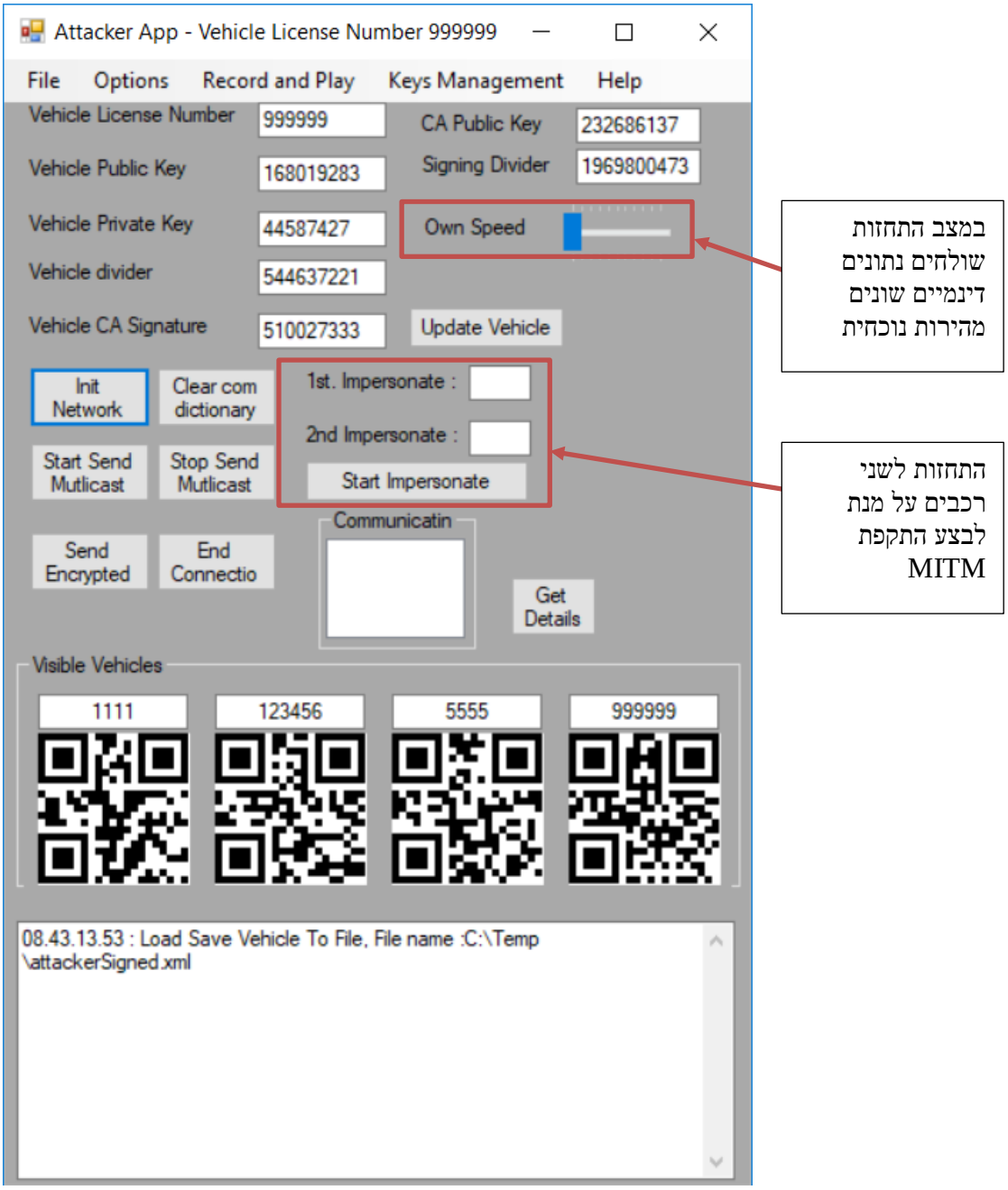




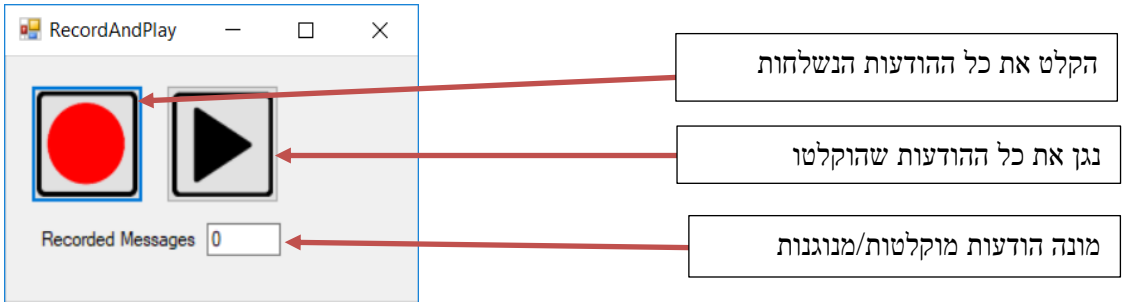
איור 23 : ממשק משתמש אפליקציית Vehicle פקודות נוספות

מסכי אפליקציית Attacker

אפליקציית Attacker כוללת את כל היכולות של אפליקציית Vehicle וכן את האפשריות הבאות המתוארות באיורים מס' 24 ו 25 .



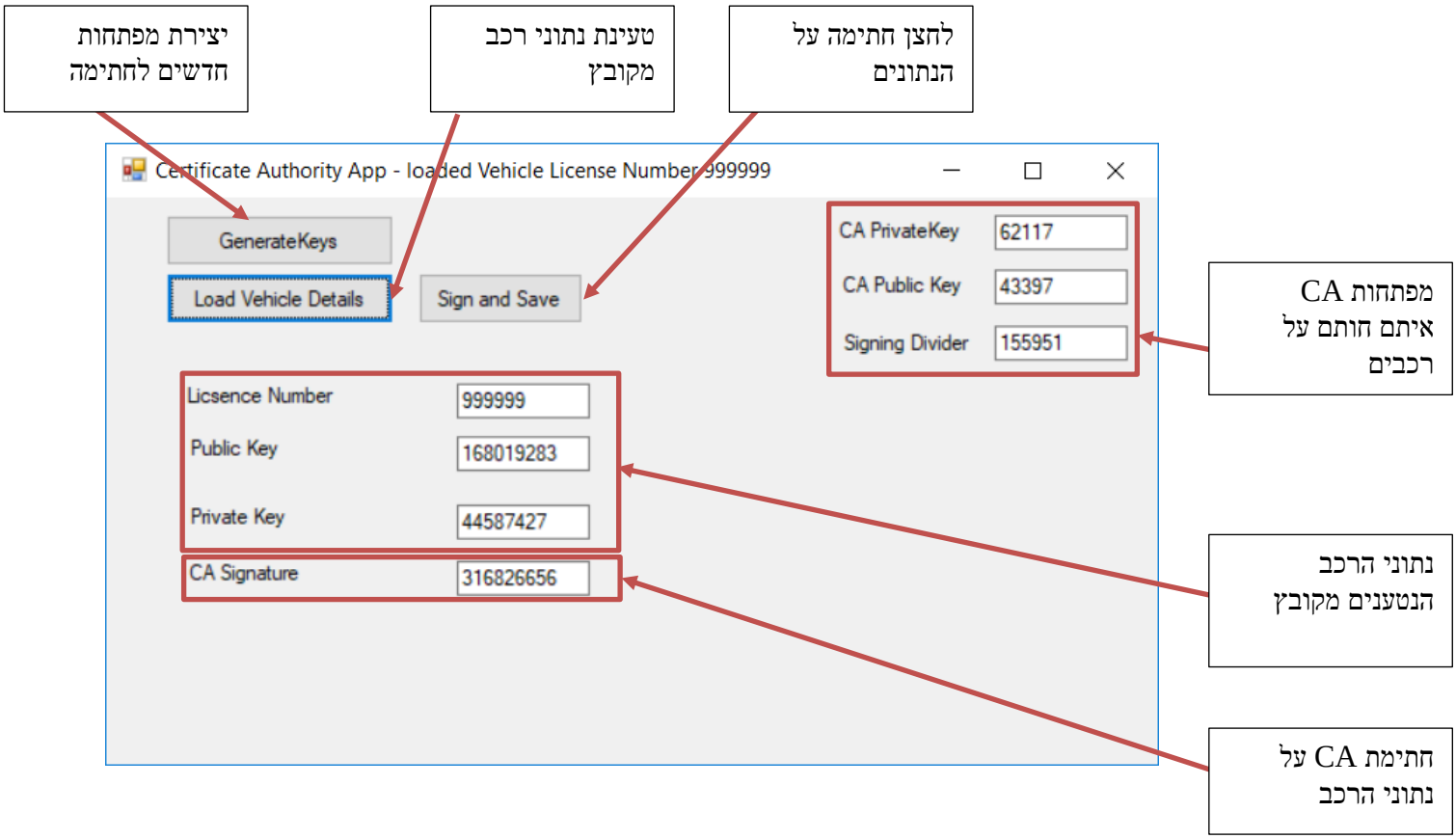
איור 24 : ממשק משתמש אפליקציית Attacker



איור 25 : ממשק משתמש אפליקציית Attacker הקלטה וניגון הודעות

מסכי אפליקציית Certificate Authority

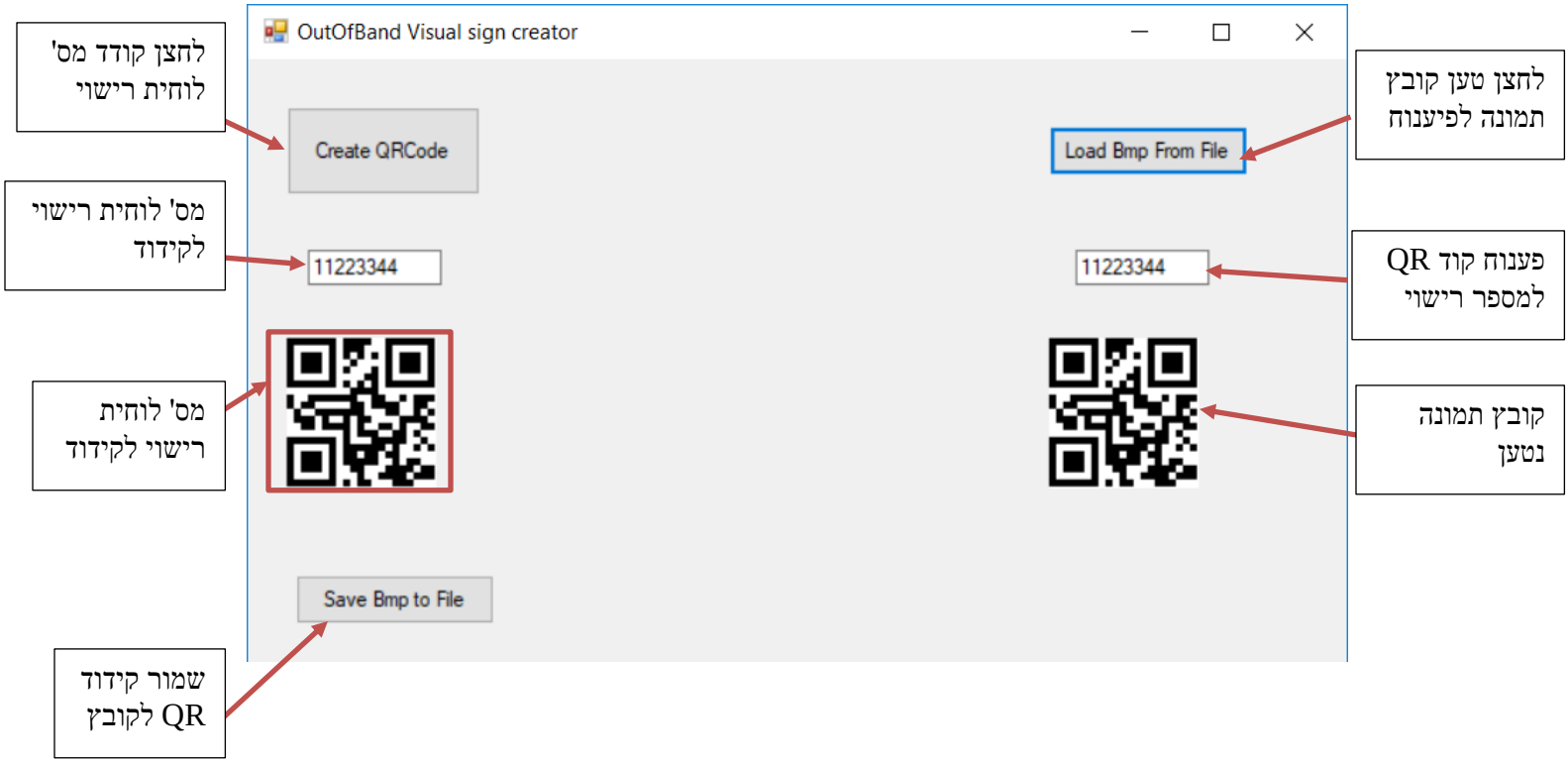
ראה איור מס' 26.



איור 26 : ממשק משתמש אפליקציית Certificate Authority

מסכי אפליקציית Out Of Band Visual sign (QR Code) Creator

ראה איור מס' 27.



איור 27 : ממשק משתמש אפליקציית Visual Sign creator