פרק א – ייזום

תיאור ראשוני של המערכת

## תקציר כולל ורציונל הפרויקט

הרשת היא איננה מקום בטוח, בקלות יחסית יכול כל אחד להאזין לערוצי תקשורת ולהתבונן במסרים העוברים בהם. לכן, קיים צורך להעביר בצורה מתוחכמת יותר הודעות עליהן אנחנו רוצים לשמור בסוד - כך שעבור אדם המביט על זרם התקשורת מהצד, הוא לא יראה כמו יותר מג'יבריש. את הבעיה הזו באה המערכת לפתור, בשימוש בהצפנה מקצה לקצה ובשיטות הצפנה אסימטריות מתקדמת (RSA לדוגמה) שמה לה למטרה המערכת לאפשר שליחת מסרים מוצפנים לגמרי. המערכת תתמוך בשיחות קבוצתיות ואישיות בהן יוכלו להישלח קבצים ומסרים , מלווים באפשרות ל-"השמדה עצמית" – כלומר מחיקת המסר את תוך זמן הנבחר על ידי המשתמש.

## המוצר המוגמר

המוצר המוגמר צריך להיות מסוגל לאפשר למשתמש, אחרי תהליך זיהוי, לשלוח מסרים בצ'אט אישי וקבוצתי כך שיגיעו ליעדם בצורה ברורה ובו בזמן לא יהיו חשופים לעין זרה במהלך מסעם ברשת האינטרנט, בדרך בין לקוח ללקוח.

## למה בחרתי בפרויקט ומה האתגרים שאני צופה לי בפרויקט

בחרתי בפרויקט משם שאני מאמינה כי פרטיות המידע היא עניין שאין להקל בו והשכיחות הגבוהה של פעולות גניבת מידע, סחיטה וכו' יכולות להיפתר בעזרת תקשורת מוצפנת.

בנוסף, רציתי להתמודד עם האתגרים שמזמן הפרויקט, ועם הרקע התיאורטי שהוא דורש – הצפנה אסימטרית, אלגוריתמיקה של הצפנת RSA , טכניקות שונות ל – "גניבת מידע" – בהן אשתמש לבדיקת המערכת.

הגדרת הלקוח

## למי מיועדת המערכת ומי הולך להשתמש בה?

המערכת מיועדת לכל אדם המעוניין להעביר מסרים ללא הסיכוי שיתגלו בידיי אנשים אחרים אשר יאזינו לתקשורת. שימוש אפשרי לה הוא בקבוצות פיתוח של רעיונות חדשניים – דוגמת סטארט אפים, המעבירים ביניהם מידע רגיש שאסור שייפול לידי מתחריהם. בנוסף, ארגונים המתמודדים עם מידע חסוי ורגיש של אנשים (בתי חולים, בנקים).

הגדרת יעדים/מטרות

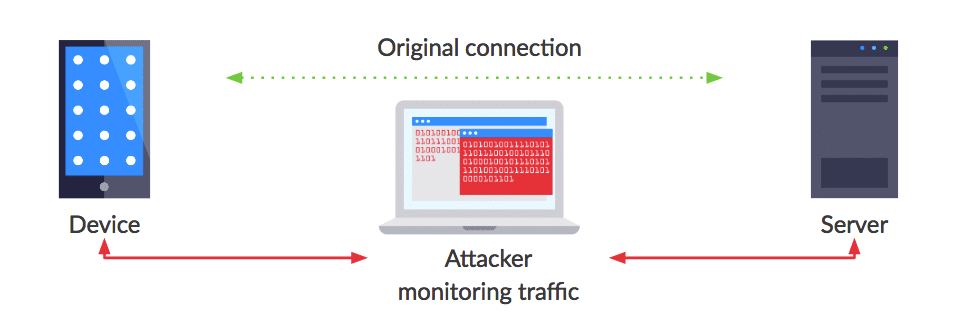
## מה המטרות המרכזיות של המערכת המוצעת (לפרט לכל לקוח ולקוח)

1. יצירת קשר מוצפן בין קבוצת לקוחות (שניים ומעלה) בשימוש בהצפנה אסימטרית והחלפת מפתחות.
2. העברת מסרים וקבצים מוצפנת ללא פגיעה במהירות או בחוויית המשתמש.
3. העברת מידע מוצפן ברשת והתמודדות עם ניסיונות הסנפה ומתקפות MITM – "אדם באמצע".

בעיות, תועלות וחסכונות

## הבעיה אותה אנחנו מנסים לפתור

מערכות תקשורת שונות לא מאבטחות ומצפינות את המידע שלהם היטב כאשר הוא עובר מאדם לאדם, ובכך משאירות אותו חשוף למתקפות MITM. מתקפת MITM (man in the middle), במתקפה זו צופה אדם בעל כוונה זדונית על זרם התקשורת בין השרת ללקוח, וגונב את המידע שנחלק ביניהם. הפרויקט מגיע כדי לפתור בעיה זו ולהשיג מערכת תקשורת ("מסנג'ר") מוצפנת לחלוטין, כך שגם אם יאזין מישהו לתקשורת המידע לא ייחשף בפניו.



איור 1 ייצוג למתקפת "אדם באמצע".

## מה התועלות שסביר לצפות מהמערכת?

המערכת תשמור על סודיות המידע העובר ברשת ופרטיות המשתמש. תאפשר לאנשים לשוחח לא חשש כי אדם או גוף חיצוני מאזין לשיחותיהם.

## אלו שירותים המערכת תיתן?

המערכת תאפשר למשתמש צ'אט פרטי (שני אנשים) וקבוצתי בו יוכל לשתף הן במסרים (הודעות טקסט) והן בקבצים. כאשר יצטרף אדם למערכת ויזדהה, יוכל לבחור מי מאנשי הקשר שלו, במידה ויצטרפו למערכת (או שהם כבר נמצאים בה), יוכל לראות שהוא חלק ממנה. השיחות האישיות יוכלו להתבצע רק מתוך מאגר זה והמערכת לא תכריז על הצטרפות של משתמש חדש לאנשי הקשר שלו.

השוואת העבודה עם פתרונות ויישומים קיימים   
Telegram – מאפשרת גם היא העברת מסרים מוצפנים בשיטת end to end encryption מלקוח ללקוח, טלגרם מאפשרת ללקוחות לנהל את השיחות ללא גיבוי בשרת אך כברירת מחדל המידע המוצפן נשמר בשרתיה ברחבי העולם. בשונה מהמערכת הנוכחית, כל אדם המצטרף אליה יכול לראות מי מאנשי הקשר שלו נמצא בה ומי לא, כך שפרטיותם של האנשים לא נשמרת במלואה. יתר על כך, הצטרפות למערכת משמעה הפצת הודעה לכל אנשי הקשר של המשתמש, המכריזה על הצטרפותו.   
קיימות מערכות דומות נוספות (Viber, KakaoTalk Dust) הממשות גם הן הצפנה מקצה לקצה בשיטות שונות.

האם צפויים קשיים או מגבלות בהגדרת המערכת

## האם מדובר בטכנולוגיה חדשה ובלתי מוכרת?

העברת מסרים מוצפנים בשימוש בהצפנת קצה לקצה הינה שיטה מוכרת יחסית, יחד עם זאת הפרויקט ימצא מקום לחידושים טכנולוגיים בשיטות ההצפנה והדקויות בתוכן.

סייגים בהגדרת המערכת   
בשונה משרתי הענק של טלגרם ואפליקציות דומות, המערכת הנוכחית לא תוכל לתמוך בכמות גדולה מאוד של לקוחות אלא במדגם מצומצם יחסית.

תיחום הפרויקט

הפרויקט במהותו עוסק בתקשורת רשתית ותתבצע בו תקשורת דרך sockets בין משתמשים ושרת/ים. בנוסף, ימומשו אלגוריתמי הצפנה מורכבים לצורך הסתרת המידע העובר ברשת. יתבצעו בדיקות רשתיות (דוגמת הסנפה) על מנת לבדוק את הפרויקט בשלביו השונים. מעבר לקשר שבין מחשב למחשב, ישתמש במערכת ההפעלה, הן בהרצת תהליכים במקביל ותקשורת ביניהם והן בשימוש בפונקציות המערכת על מנת למחוק בצורה סופית קובץ. המערכת לא תעסוק בפן האתי של תקשורת מוצפנת. ולא תתערב בתוכן המידע המועבר בה (לא תגביל מילים מסוימות וכדומה).

פרק ב' אפיון

פרוט המערכת

הרשת היא איננה מקום בטוח, בקלות יחסית יכול כל אחד להאזין לערוצי תקשורת ולהתבונן במסרים העוברים בהם. לכן, קיים צורך להעביר בצורה מתוחכמת יותר הודעות עליהן אנחנו רוצים לשמור בסוד - כך שעבור אדם המביט על זרם התקשורת מהצד, הוא לא יראה כמו יותר מג'יבריש. את הבעיה הזו באה המערכת לפתור, בשימוש בהצפנה מקצה לקצה ובשיטות הצפנה אסימטריות מתקדמת (RSA לדוגמה) שמה לה למטרה המערכת לאפשר שליחת מסרים מוצפנים לגמרי. המערכת תתמוך בשיחות קבוצתיות ואישיות בהן יוכלו להישלח קבצים ומסרים , מלווים באפשרות ל-"השמדה עצמית" – כלומר מחיקת המסר תוך זמן הנבחר על ידי המשתמש.   
למעשה כדי לצמצם כמה שאפשר את התלות בשרת הוא יהווה מעין "מחזיק מפתחות" ויספק למשתמש מסוים את המפתח הציבורי של המשתמש אתו הוא רוצה לשוחח, משם תתקיים תקשורת peer2peer בין שני המשתמשים בלי תלות בשרת.   
המוצר המוגמר צריך להיות מסוגל לאפשר למשתמש, אחרי תהליך זיהוי, לשלוח מסרים בצ'אט אישי וקבוצתי כך שיגיעו ליעדם בצורה ברורה ובו בזמן לא יהיו חשופים לעין זרה במהלך מסעם ברשת האינטרנט, בדרך בין לקוח ללקוח.

יכולות המערכת

* 1. שליחת מסרים מוצפנים - התנהלות מהירה ברשת תוך כדי שמירה מקסימלית על פרטיות המשתמש.
  2. העברת קבצים ברשת.
  3. שיחות פרטיות – אפשרות ליזום שיחה פרטית ולהשתתף באחת.
  4. Peer2Peer – התקשורת בין הלקוחות תתבצע ללא תלות בשרת לאחר החלפת המפתחות הציבוריים.
  5. שיחות קבוצתיות בין משתמשים – אפשרות ליזום שיחה קבוצתית ולהשתתף באחת.
  6. ממשק משתמש נגיש ונוח לשימוש
  7. חשיפת מידע מינימלית
     1. לא יופץ מידע על הצטרפות אדם חדש למערכת.
     2. אפשרות לחסום משתמשים מסוימים מלצפות בסטטוס החיבור של המשתמש עצמו.

בדיקות קופסא שחורה

| מספר | שם הבדיקה | מה אמורה לבדוק | תכנון הבדיקה |
| --- | --- | --- | --- |
|  | הסנפה | האם המידע העובר ברשת יהיה חשוף לאדם הצופה בזרם התקשורת של המערכת. | בבדיקה נדמה את מתקפת MITM ממנה אנחנו מנסים להגן על המשתמש. נפעיל תוכנת הסנפה (Sniffer) בזמן אמת כאשר ישנם משתמשים המחוברים למערכת ושולחים בה מסרים. נעצור את ההסנפה נצפה בפקטות ונראה האם ניתן לקשר ביניהן לתוכן ההודעות שנשלחו ללא מידע נוסף. |
|  | תקינות שיחה | האם כל המידע שנשלח ממשתמש אחד מגיע למשתמש אליו הוא נשלח (צ'אט פרטי וקבוצתי). | נשלח מסרים מלקוח ללקוח ונשווה בין המידע שנשלח לזה שהתקבל. |
|  | העברת קבצים | האם קבצים שנשלחו הגיעו במלואם ובצורה תקינה המאפשרת פתיחה | נשלח קבצים בין המשתמשים וננסה לפתוח אותם. |
|  | הצפנת מידע ופיענוחו | האם תהליך ההצפנה לא פוגע במידע עצמו, האם המידע מוצפן כראוי | השוואה בין המסר שנשלח לבין המסר שהוצג ללקוח (פיענוח של המסר המוצפן) |
|  | ניהול שיחות במקביל | האם השרת מצליח לתמוך בניהול של כמה שיחות קבוצתיות ופרטיות באותו הזמן, ללא עיכובים. | ננהל כמה שיחות באותו הזמן, נמדוד את זמני התגובה של השרת ונצפה האם יש מגמת עלייה משמעותית בזמן התגובה עבור כמה שיחות במקביל |
|  | יציבות השרת | האם השרת יציב ולא קורס במהלך הרצת המערכת. | הרצת המערכת, טיפול בבקשות התנתקות והתחברות של לקוחות. טיפול וניסיון לחזות שגיאות. |
|  | צ'אט קבוצתי | האם השרת מצליח לתמוך בצ'אט קבוצתי ולדאוג שהמידע יהיה חשוף רק למשתמשים הנמצאים בקבוצה. | יצירת קבוצה ומשתמשים נוספים, בדיקה האם המידע ראשית, מגיע לכל המשתתפים בשיחה, שנית לא מגיע למשתמשים אחרים. |
|  | הזדהות משתמשים | האם השרת מצליח לזהות כל משתמש בעזרת שם המשתמש והסיסמה שהגדיר | יצירת משתמשים וניסיון לגשת לחשבונם ללא המידע המלא הדרוש לכך לעומת ניסיון לגשת לחשבונם עם שם המשתמש והסיסמה התקינים. |
|  | השמדה עצמית | האם המנגנון עובד כנדרש. | ביצוע השמדה עצמית של קובץ וניסיון למציאת שאריות שלו במחשב – בסל המחזור לדוגמה. |
|  | חשיפה | האם הצטרפותו או התחברותו של משתמש חדש למערכת ידועה לשאר המשתמשים. | התחברות למערכת מצד משתמש אחד ובדיקת ההשפעה על המידע הנגיש לשאר המשתמשים. |

תכנון לוח זמנים לפרויקט

| פעילות | זמן התחלה מתוכנן | זמן סיום מתוכנן | זמן התחלה בפועל | זמן סיום בפועל | הערות |
| --- | --- | --- | --- | --- | --- |
| הגשת מסמך הייזום | 29/11/18 | 5/12/19 | 11/11/19 | 18/11/19 | הקדמתי את לוח הזמנים בחודש. |
| הגשת מסמך האפיון | 19/12/18 | 24/12/18 | 18/11/19 |  |  |
| הגשת מסמך הניתוח | 19/01/18 | 24/01/18 |  |  |  |
| הגשת מסמך העיצוב | 25/01/19 | 12/02/19 |  |  |  |
| בניית חבילה לפעולות ההצפנה | 12/02/19 | 19/02/19 |  |  |  |
| יצירת ממשק משתמש - לקוח | 19/02/19 | 25/02/19 |  |  |  |
| שיחה בין שני משתמשים | 25/02/19 | 31/02/19 |  |  |  |
| שיחה קבוצתית | 31/02/19 | 03/03/19 |  |  |  |
| העברת קבצים | 03/03/19 | 09/03/19 |  |  |  |
| השמדת קבצים | 09/03/19 | 11/03/19 |  |  |  |
| הגשה ראשונית של הפרויקט | **12/03/19** |  |  |  |  |
| שיפור החלקים השונים הקיימים | 12/03/19 | 24/03/19 |  |  |  |
| הגשת מסמך ההטמעה – מדריך למשתמש | **25/03/19** |  |  |  |  |
| הגשה סופית - תיק פרויקט וקוד גמור | **30/03/19** |  |  |  |  |

ניהול סיכונים בפרויקט

| הסיכון | פירוט הסיכון | רמת הסיכון  (קל/בינוני/קשה) | דרכים להתמודדות עם הסיכון ולהקטין אותו | מה בוצע בפועל | תאריך |
| --- | --- | --- | --- | --- | --- |
| פריצה של ההצפנה | חשיפת המידע במסר | קשה | בחירה באלגוריתם הצפנה שנחשב בלתי חדיר (RSA).  העברה של מידע חיוני ברשת, רק כשהוא מוצפן. |  |  |
| אי עמידה בלוח הזמנים | עיכוב בלוח המזנים יגרור עיכוב בכל שאר החלקים | קשה | הגשת כל חלק בזמן.  מניעה של פתיחת פערים גדולים מידי.  הקדשת שעות נוספות. |  |  |
| קריסה של השרת | קריסה של השרת תסכן את פרטי המשתמשים | קשה | לא יישמר אצל השרת מידע רב, השרת למעשה רק ינהל מפתחות. לאחר שקיבל זוג משתמשים זה את מפתחו הציבורי של זה, הם לא זקוקים לשרת יותר.  מניעת עומס יתר על השרת, תיעדוף משימות מסוימות על אחרות.  כתיבת קוד בטוח ומוגן. |  |  |
| שימוש בממשק הגרפי | בניית מסכים נוחים למשתמש | קשה | אצטרך ללמוד את המודול WXPython לפני הכתיבה. זהו מודול חדש אותו אני לא מכירה.  תכנון המסכים מראש. |  |  |
| שליחת קבצים מוצפנת | לא ריאלי להצפין קובץ שלם בתקשורת בהצפנת RSA | קשה | מציאת שיטת הצפנה אחרת, פחות מסובכת (כנראה סימטרית) להצפנת הקבצים. |  |  |
| תקשורת איטית | העברת הקבצים והמסרים בשילוב עם פיענוח והצפנת המידע תעיק על התהליך, תהפוך אותו לאיטי ותפגע בחוויית המשתמש | בינוני | תכנון ומימוש אלגוריתם יעיל ככל האפשר.  ביצוע תיעדוף משימות אצל הלקוח ואצל השרת.  פריסת המשימות על כמה תהליכים שיתבצעו במקביל. |  |  |
| העברת קבצים ומסרים | על הקבצים להגיע בצורה שלמה מהמקור ליעד | בינוני | פרוטוקול שליחה בחלקים ואישור אחרי כל חלק.  מעקב אחר העברת הקובץ או המסר ולא שליחתו בפעם אחת. |  |  |