מטלת סיום בקורס תקשורת

מגישים:

שם: מסנבט מולו ת"ז : 319311940

שם: אהרון לוחן ת"ז : 336389515

קישור לפרויקט : https://github.com/aronl096/Final_Project_Networks

הרעיון המרכזי

הרעיון המרכזי של המאמר הוא להדגיש חולשה חשובה ביישומי מסרים מיידיים פופולריים כמו טלגרם, סיגנל ו-WhatsApp. למרות שהם משתמשים בטכנולוגיות הצפנה מתקדמות, המאמר מראה שהם עדיין פגיעים להתקפות של ניתוח תעבורה. ההתקפות מאפשרות ליריבים, כמו ממשלות המבצעות סינון ומעקב, לאסוף מידע רגיש על פעילות המשתמשים בתוך הפלטפורמות.

בעצם העלאת המודעות לגבי האבטחה של האפליקציות הללו.

החוקרים מדגישים שהתקפות אלו אינן נובעות משימוש בחולשות תוכנה, אלא מתוך החולשה בשיטות להסתיר תנועה שנעשה בשירותי ה .IM-על ידי ניתוח תכונות של תנועת הודעות מוצפנות, כמו זמני החבילות וגודלן, יריבים יכולים לזהות חברים ומנהלים בערוצים מסוימים ברמה גבוהה של דיוק.

המאמר מדגיש את ההשלכות המעשיות של התקפות אלו, בעיקר באזורים בהם משטרים אכפתיים מניטור ושליטה בתקשורות שנעשות על נושאים רגישים. החוקרים מקווים שהממצאים יעוררו את ספקי שירותי ה IM-להשתמש באמצעים יעילים להסתיר תנועה. בינתיים, הם מציעים פתרון קוד-פתוח שנקרא ,IMProxy שמשתמשים יכולים להשתמש בו כדי להגן על עצמם מהתקפות ניתוח תנועה אלו.

כיצד משיג התוקף ground truth על תעבורת הערוץ?

התוקף משיג " תשתית אמת " של התעבורה בערוץ ה IM-היעד על ידי כלל הופעה בשימוש מסוים בשיטות רבות לאספקת נתוני התקשורת באותו ערוץ. חשיבותה של האמת היא בעיקרה לצורך השוואה ותיאום בין התעבורה המותאמת לערוץ היעד לבין הדפוסים האמיתיים הנמצאים בערוץ זה. המאמר מתאר שלושה דרכים עיקריות שבהן התוקף יכול לרכוש "תשתית אמיתית" :

1) הצטרפות לערוץ כחבר: במקרה שבו ערוץ ה IM-היעד פתוח או מוגבל, התוקף יכול להצטרף אליו כחבר. באמצעות השתתפותו בערוץ, התוקף יכול לקבל גישה להודעות הממשיות, לגלות נתוני מטא (כמו הזמנים וגדלי ההודעות), ולאתר את הדפוסים התקשורתיים בערוץ. הגישה הזו מאפשרת לו לבחון בצורה ישירה את הדפוסים האמיתיים של התקשורת.

2) רכישת הרשאות פרסום בערוץ: במקרים מסוימים, התוקף יכול לרכוש הרשאות פרסום בערוץ ה IM-היעד. המצבים האלו יכולים להתרחש אם הערוץ הוא קבוצה סגורה המאפשרת לכל משתמש לפרסם הודעות, או אם התוקף מצליח להפוך למנהל של הערוץ. על ידי האפשרות לפרסם הודעות, התוקף יכול ליצור דפוסי תנועה ספציפיים על ידי שליחת הודעות עם נתוני זמנים וגודל ברורים. זה מעניק לו שליטה על התוכן והזמנים של ההודעות, ומאפשר לו ליצור את התעבורה לפי דרישותיו.

3) זיהוי חבר/מנהל: אם התוקף אינו יכול להצטרף לערוץ באופן ישיר, עשוי להיות לו אפשרות לזהות משתמש או מנהל בערוץ ה IM-היעד. פעם שהוא מזהה משתמש כזה שחלק מהערוץ, הוא יכול "להאזין" לתעבורה המוצפנת שנשלחת על ידו. על ידי התחקיר אחרי התנועה של המשתמש, התוקף יכול לראות את הדפוסים התקשורתיים שקשורים לפעילותיו בערוץ. הזיהוי העקיף הזה מאפשר לו לראות את הדפוסים האמיתיים בערוץ בלי שהוא יכול להיכנס לתוכו.

לסיכום, התוקף מצליח לרכוש את תשתית האמת על ידי השתתפות כחבר בערוץ, רכישת הרשאות פרסום, או זיהוי חברים או מנהלים בערוץ. האמת הקרקעית משמשת כבסיס לפיתוח אלגוריתמים לניתוח התעבורה המאפשרים התאמה בין התעבורה המיועדת לערוץ לבין הדפוסים האמיתיים בו.

כיצד התוקף מבצע האזנת סתר בתעבורת הרשת?

האזנת סתר מתייחסת לפעולת יירוט וניטור תעבורת תקשורת בין שני צדדים ללא ידיעתם או הסכמתם. בהקשר של תקשורת רשת, האזנת סתר כרוכה בדרך כלל בתפיסת מנות נתונים כשהן חוצות את תשתית הרשת. להלן כמה שיטות נפוצות שתוקף עשוי להשתמש כדי להשיג זאת:

א) ניטור רשת פסיבי: התוקף מגדיר ציוד ניטור, כגון הסנפת מנות, בקטעי רשת שבו עוברת תעבורת משתמש היעד. ציוד זה לוכד עותקים של מנות נתונים כשהן זורמות ברשת. ניתן לעשות זאת ברשת פיזית על ידי חיבור לרכז או על ידי הגדרת מתג רשת לשיקוף תעבורה לתחנת הניטור של התוקף.
ב) נקודת גישה נוכלת: אם משתמש היעד מחובר לרשת אלחוטית, התוקף יכול להגדיר נקודת גישה נוכלת בשם דומה לרשת הלגיטימית. כאשר המכשיר של משתמש היעד מתחבר לנקודת הגישה הסוררת, התוקף יכול ליירט וללכוד את תעבורת הרשת.
ג) תוכנה זדונית: התוקף עלול לסכן את המכשיר של משתמש היעד באמצעות תוכנה זדונית הלוכדת ושולחת עותקים של תעבורת רשת לשרת של התוקף. הדבר עשוי להיות כרוך בהדבקה של מכשיר המשתמש בתוכנות ריגול או בסוס טרויאני.
ד) ברזי רשת: בהגדרות רשת פיזיות, התוקפים עשויים להשתמש בחומרה מיוחדת המכונה ברזי רשת. התקנים אלה מוכנסים בשורה בין כבלי רשת ולוכדים באופן פסיבי תעבורה למטרות ניטור.
ה) התקפות Man-in-the-Middle (MitM): תוקף יכול למקם את עצמו בין משתמש היעד לשרת הרשת, ליירט ולהעביר תעבורה. זה מושג לעתים קרובות באמצעות טכניקות כמו זיוף ARP או זיוף DNS.
ו) יירוט בתשתית רשת: תוקפים מתוחכמים עלולים לסכן נתבי רשת, מתגים או רכיבי תשתית רשת אחרים כדי ללכוד תעבורה כשהיא עוברת דרך מכשירים אלה.

השיטות שהוזכרו לעיל הן רק כמה דוגמאות לאופן שבו תוקף עלול ליירט תעבורת רשת. השיטה הספציפית שבה משתמש התוקף יכולה להיות תלויה בערוצי התקשורת הממוקדים, ביכולות הטכניות של התוקף ובאמצעי האבטחה הקיימים כדי להגן על הרשת.

נתאר את המסקנות מטבלה II :

המאמר מדבר על התפלגות סוגי הודעות שונים בתעבורת מסרים מיידיים (IM), בניית מודלים של עיכובים בין הודעות (IMD), וזמן השהיית תקשורת של תעבורת IM.

להלן הסבר תמציתי של המידע שסופק לנו:

טבלה II: התפלגות סוגי הודעות שונים:

Type	Count	Volume (MB)	Size range	Avg. size
Text	12539 (29.4%)	3.85 (0.016%)	1B-4095B	306.61B
Photo	20471 (48%)	1869.57 (0.765%)	2.40Kb-378.68Kb	91.33KB
Video	6564 (15.4%)	232955.19 (95.3%)	10.16Kb-1.56Gb	35.49MB
File	903 (2.1%)	47.46 (0.019%)	2.54Kb-1.88Mg	52.56KB
Audio	2161 (5.1%)	9587.36 (3.92%)	2.83Kb-98.07Mg	4.44MB

עיכובים בין הודעות (IMD) וגדלי הודעות:

IMDs מתייחסים לפערי הזמן בין הודעות IM עוקבות.

IMDs קצרים מאוד מתמזגים מכיוון שהם יוצרים פרץ תעבורה שלא ניתן להפריד על ידי ניתוח תעבורה.

פונקציית צפיפות ההסתברות עבור IMDs מתאימה להתפלגות אקספוננציאלית.

הודעות נשלחות באופן עצמאי בערוצים, מה שמוביל להתנהגות אקספוננציאלית ב-IMDs.

IMDs נחשבים בלתי תלויים בסוג ובגודל ההודעה מכיוון שאין מתאם מעשי בין זמן שליחת ההודעה לסוג או גודלה.

גדלי הודעות:

מודל שרשרת מרקוב של חמש מדינות נוצר בהתבסס על הסטטיסטיקה האמפירית מטבלה II כדי לחזות את הגדלים של הודעות עתידיות.

מטריצות מעבר של מודל זה יכולות להשתנות מעט עבור ערוצי IM עם קצבי הודעות יומיים שונים.

לסוגי הודעות שונים יש התפלגות גודל הודעה ברורה.

אחזור תקשורת:

עיכובים בהודעות IM מיוחסות לאחזור רשת ולאחזור עיבוד שרת IM.

תעבורת IM מ-500 ערוצים (מעל 500 שעות) נאספה דרך ה-API של Telegram כדי ללמוד את ההשהיות הללו.

ההשהיות שנצפו מתאימים בצורה הטובה ביותר למודל שנגזר באמצעות הערכת סבירות מקסימלית (MLE).

הסבר זה מקיף את הסעיף שסופק על ניתוח תעבורת IM, תוך הדגשת פרטי הליבה והממצאים שניתנים לנו.

איור 8 :

ניתן לראות במאמר תרשימים של גודל הpacket בקרב שני משתמשים – אחד שלא שייך לקבוצה .

בצד התחתון של האיור ניתן לראות events שקורים במהלך פרק הזמן בו מתבוננים על תעבורת שני המשתמשים (שליחת תמונה, שליחת סרטון, שליחת קובץ אודיו, ושליחת קובץ), כאשר עבור המשתמש אשר זוהה כשייך לקבוצה – ניתן לראות שבכל שליחה שכזו יש מספר MTU (לפחות 1, בדיוק בזמן הevent), בעוד שעבור המשתמש שלא זוהה כשייך לקבוצה ישנם MTU בזמנים שונים, לא בהכרח בזמן event.

לאחר מכן, בודקים החוקרים את המודלים שלהם על טלגרם, ווטסאפ וסיגנל. הם מראים שהפעלת האלגוריתמים שלהם נותנים תוצאות זיהוי טובות וזה מהווה איום משמעותי על המשתמשים, לאור הניסיונות ההולכים וגדלים של ממשלות מדכאות לפצח את הערוצים השנויים במחלוקת בפלטפורמות הללו.. במקביל, זה גם מדגיש את הצורך של ספקי שירותים לשלב אמצעי נגד אפקטיביים של ערפול תעבורה במערכות שלהם, מעבר להצפנה בלבד, כדי להבטיח את הפרטיות והבטיחות של המשתמשים שלהם.

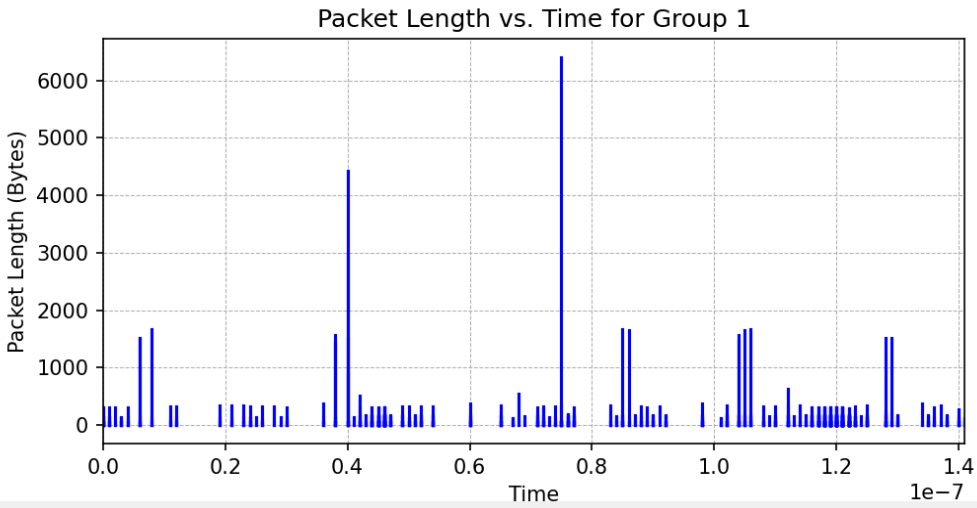
לבסוף, המחברים מציגים מערכת אמצעי נגד הנקרא IMProxy . מערכת זו נועדה להגן מפני ההתקפות מסוג זה בדיוק. החוקרים גילו כי ביצוע של tunnelling (מנהור) של תעבורת SIM דרך VPN וערבוב שלה עם תעבורת גלישה באינטרנט מפחיתה את דיוק ההתקפה באמצעות שני האלגוריתמים שלהם .

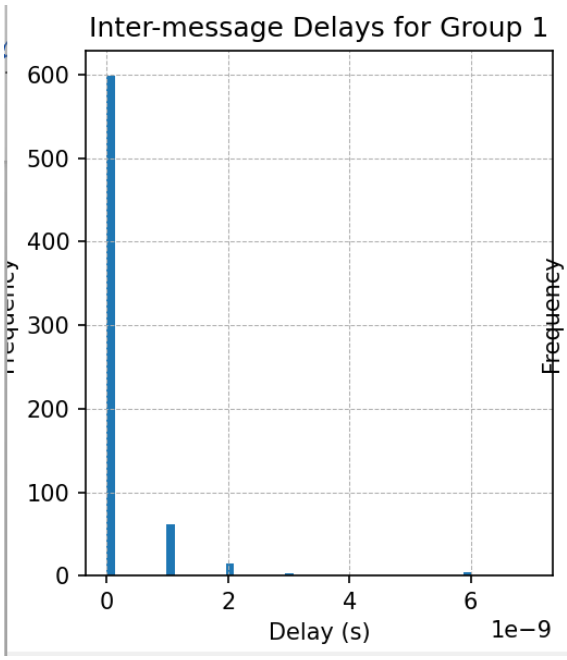
לפי הכתוב לעיל החוקרים פרסמו מערכת אמצעי נגד, הזמינה לציבור בקוד פתוח, הנקראת IMProxy, שיכולה לשמש לקוחות IM ללא צורך בתמיכה כלשהי מספקי IM, אשר מביאה לתוצאות טובות אשר הוכחו גם בניסויים.

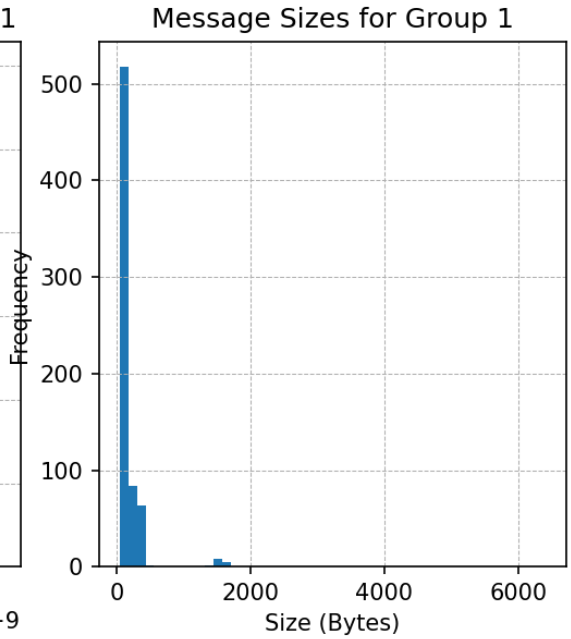
חלק רטוב :

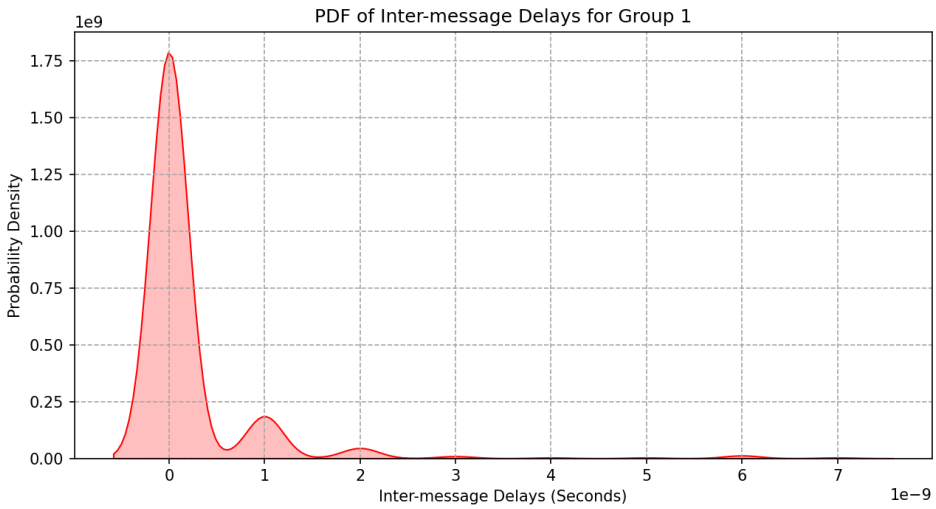
עתה נראה את הגרפים שהקוד שלנו חילץ מההקלטות pcap שלנו אשר המרנו לקבצי csv על מנת שנקבל תוצאות מדויקות יותר מהנתונים הגרף הראשון לכל קבוצה הוא של גודל הפאקטות (ציר y) על זמן (ציר x), 2 הגרפים האחרים שמופיעים לאחר מכן של אותה קבוצה הם 1) תדירות שליחת ההודעות (ציר y) על העיכוב של ההודעות(ציר x), 2) תדירות שליחת ההודעות (ציר y) על פי גודל הפאקטות שהועברו (ציר x). הצירים מותאמים בהתאם לערך המקסימלי ולערך המינימלי לכן כל גרף מותאם לקבוצה שלו.

קבוצה 1: הודעות טקסט

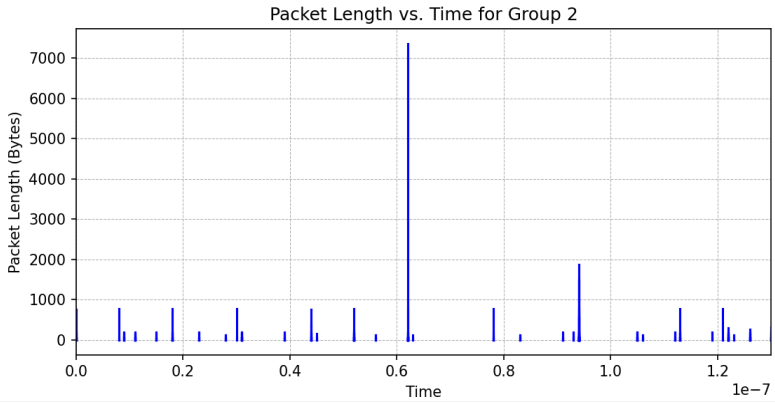


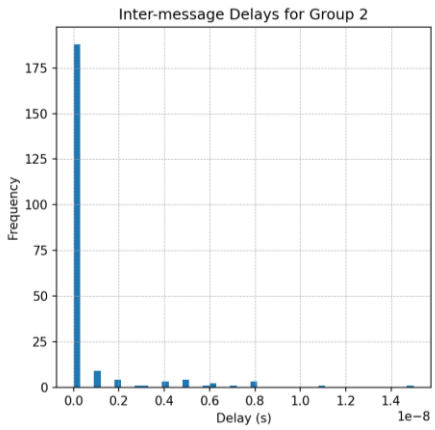


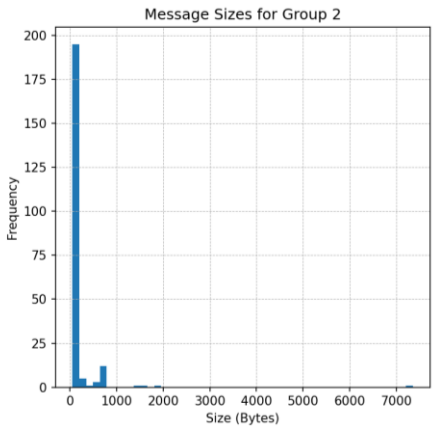


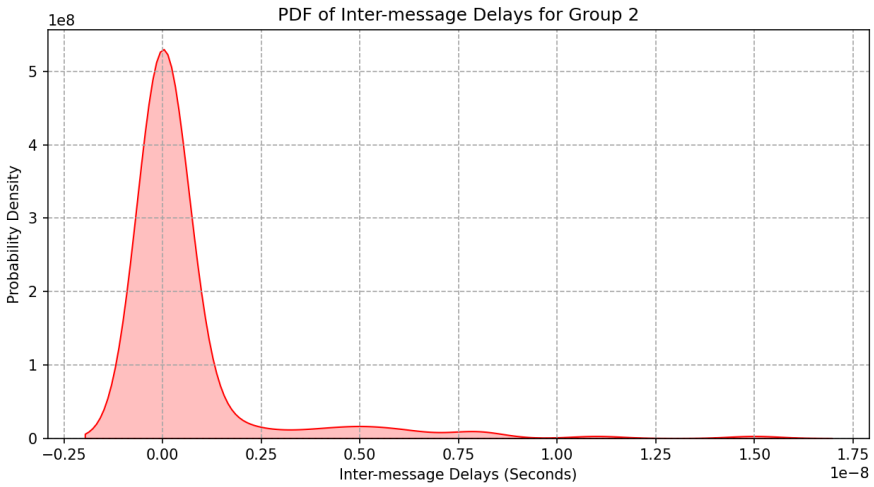


קבוצה 2: הודעות קוליות

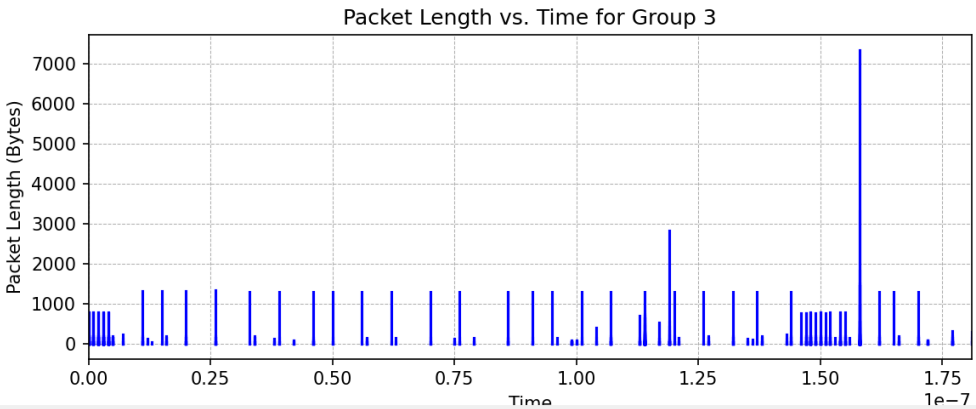


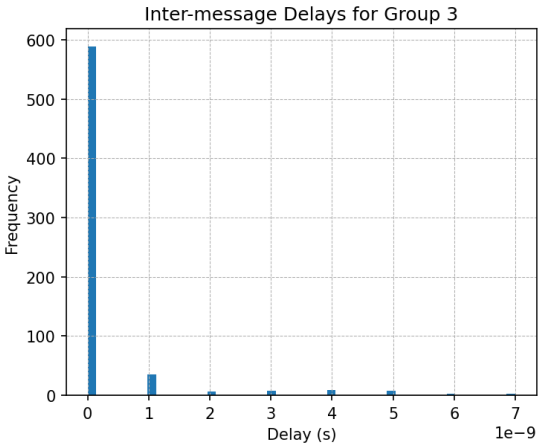


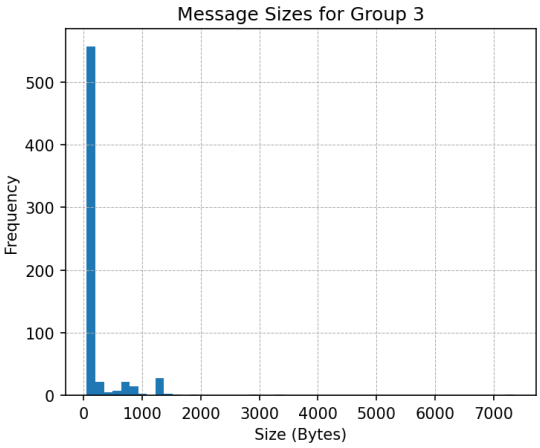


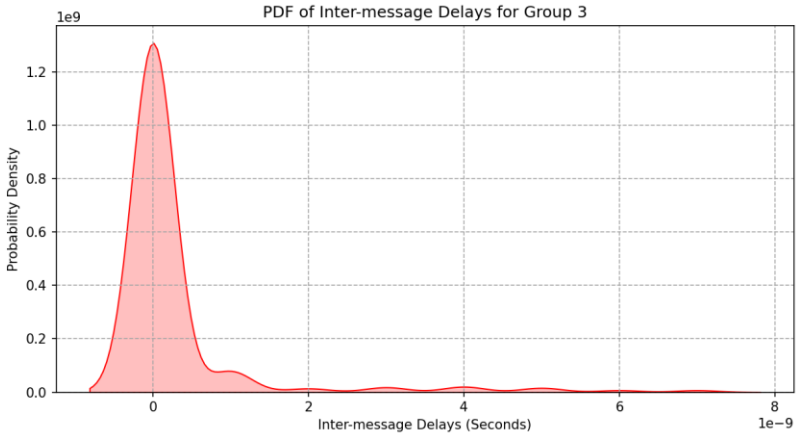


קבוצה 3: הודעות עם תמונות

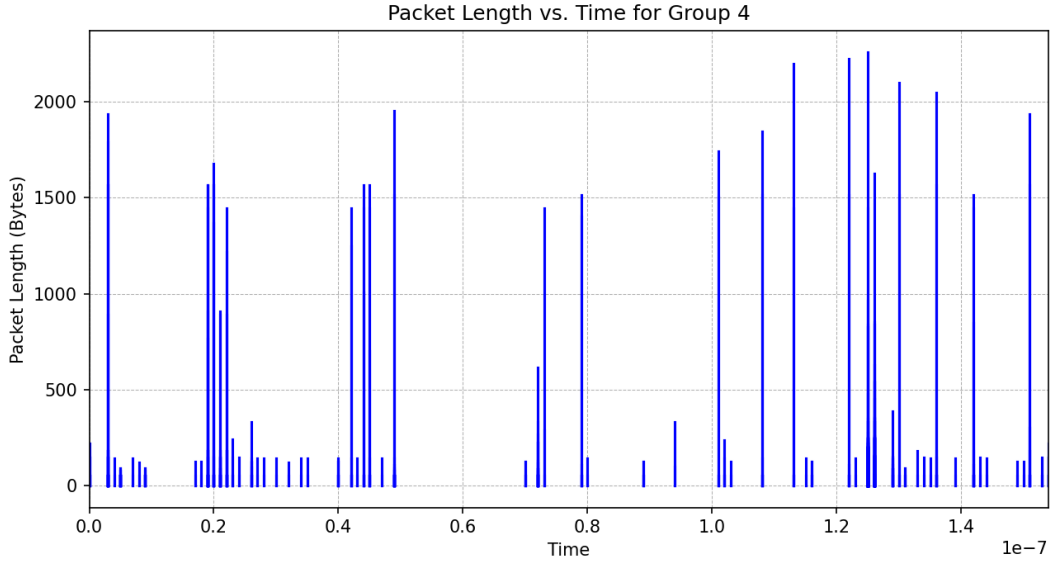


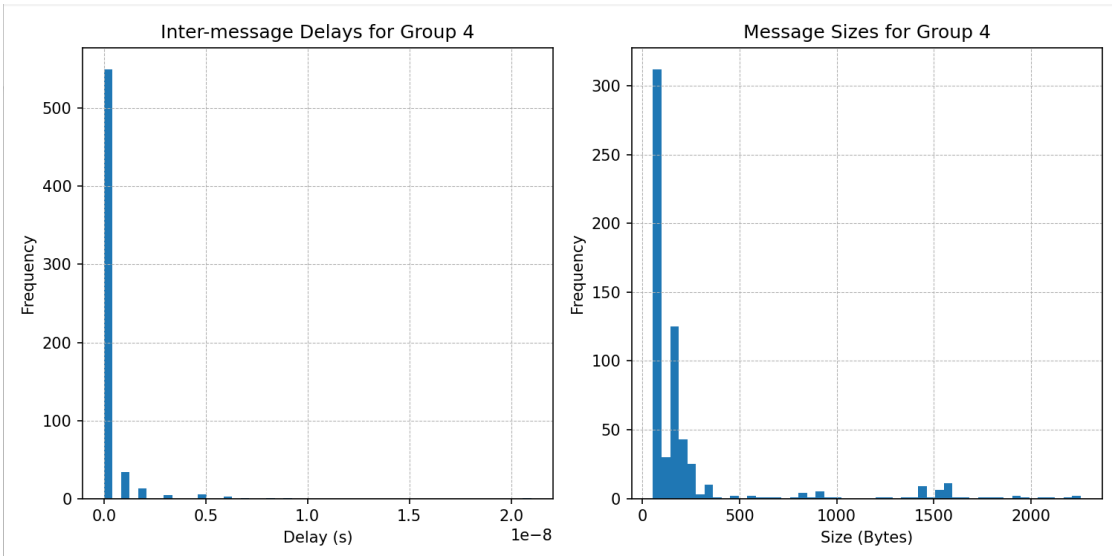


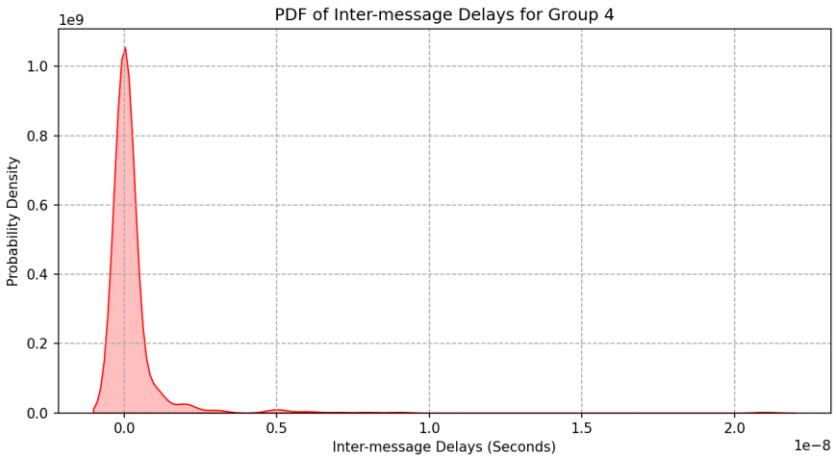




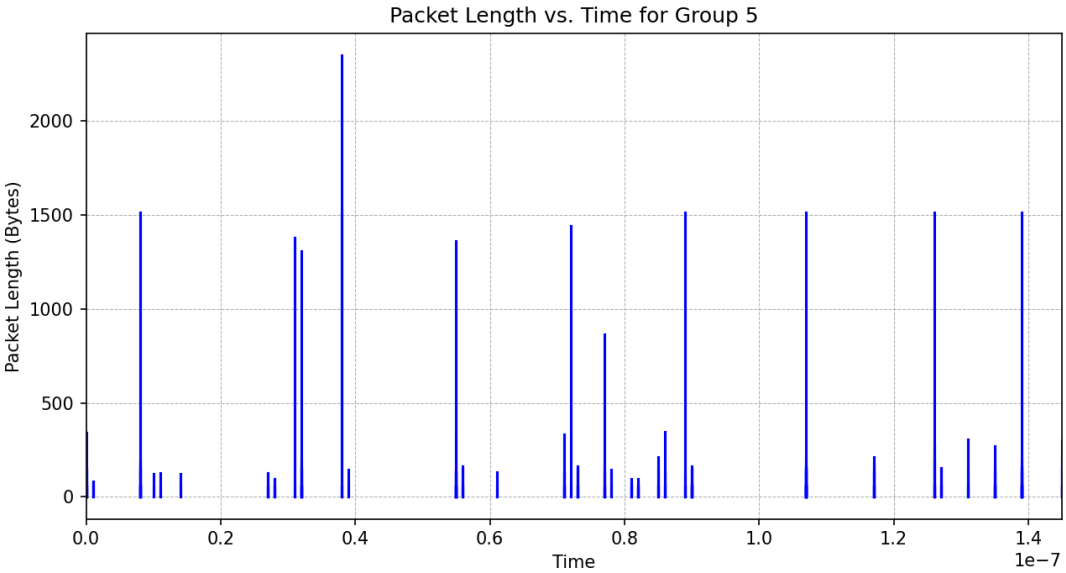
קבוצה 4:הודעות עם קבצים

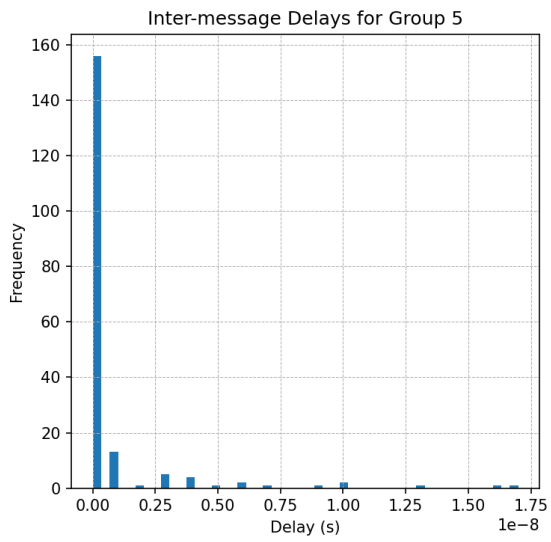


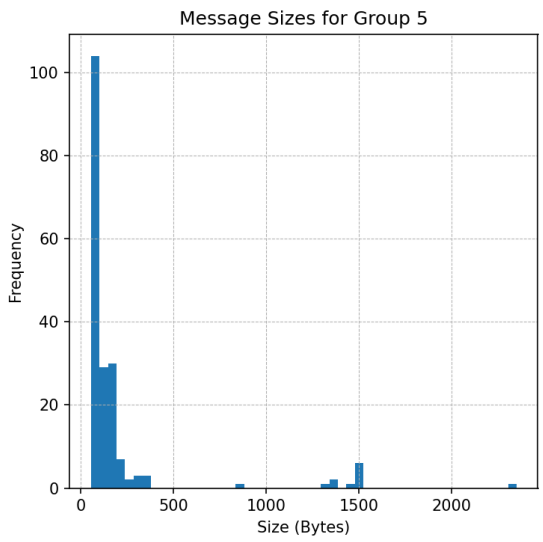


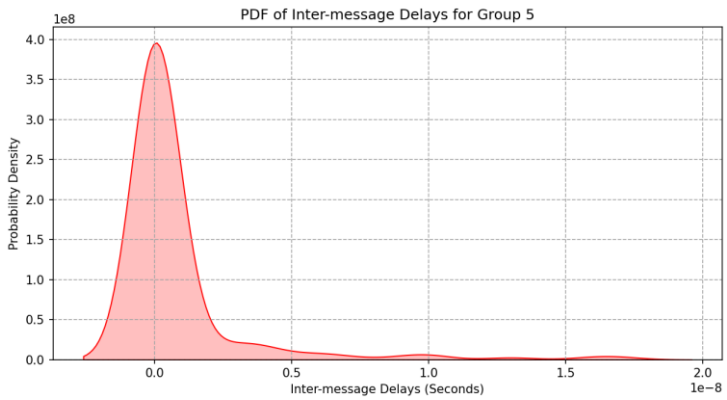


קבוצה 5:הודעות עם סרטונים

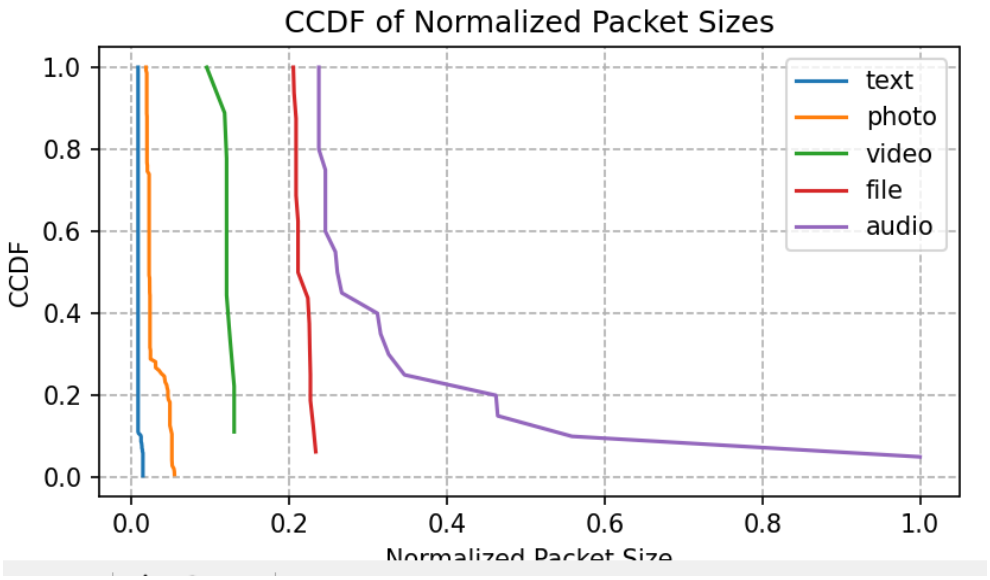








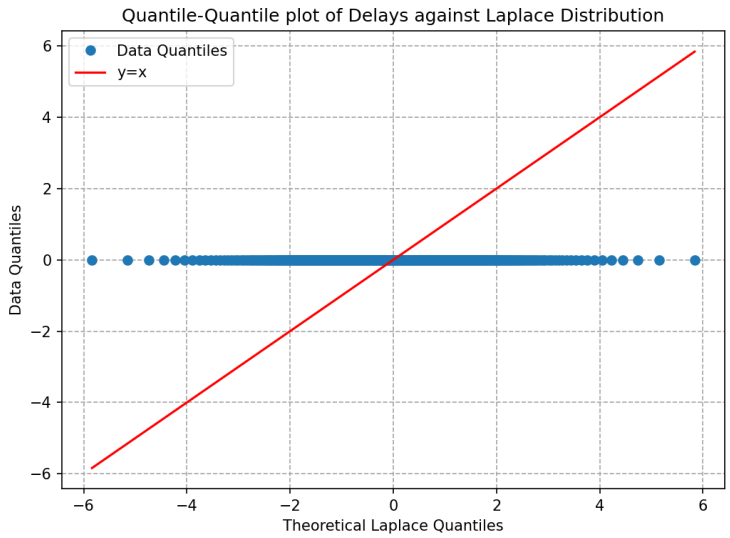
קבוצה 6 אשר היא קבוצת מיזוג של כלל הקבוצות יחד :

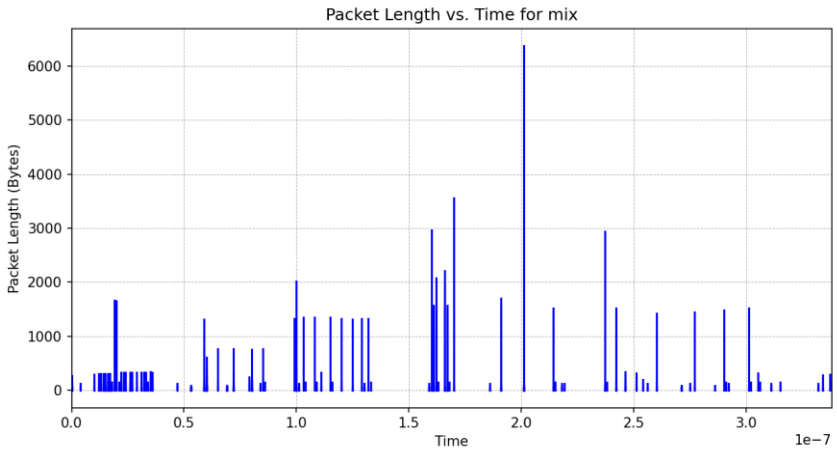


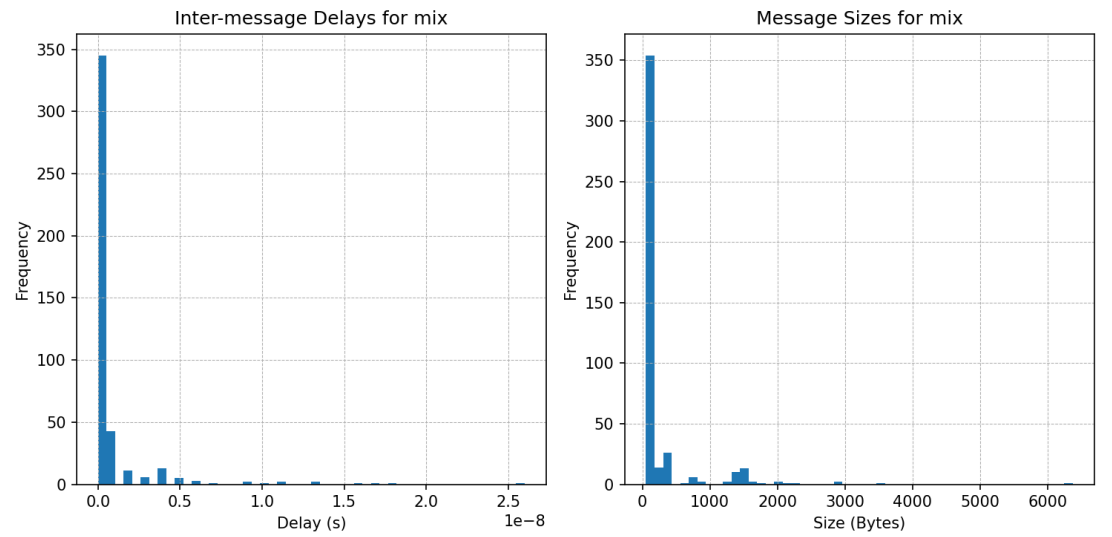
```
Number of data points for text: 252
Number of data points for photo: 142
Number of data points for video: 9
Number of data points for file: 16
```

הפונקציה אכן מתארת את ה-CCDF של פיזור גודל IM עבור סוגים שונים של הודעות.

כל קו (או עקומה) על הגרף מייצג את ה-CCDF עבור סוג הודעה ספציפי.







התמונות של אותם קבוצות עם רעשי רקע (ספוטיפיי ויוטיוב) מצורפות ל.Github

קישורים ל- github ו- LinkedIn :

https://github.com/Masanbat12

https://github.com/aronl096

/https://www.linkedin.com/in/masanbat

https://www.linkedin.com/in/aaron-luchan-a06111230/