<u>הרעיון המרכזי של המאמר:</u>

המאמר "Practical Traffic Analysis Attacks on Secure Messaging Applications" עוסק בהתקפות ניתוח תעבורה על יישומי הודעות מיידיות מאובטחים (IM) כמו Telegram, Signal ו- WhatsApp.
הרעיון המרכזי של המאמר הוא להראות שאף על פי שיישומים אלה משתמשים בהצפנה חזקה, הם עדיין חשופים להדלפת מידע רגיש על המשתמשים שלהם ליריב שפשוט מאזין לתעבורה המוצפנת.
המאמר מציג התקפות ניתוח תעבורה שמאפשרות ליריב לזהות מנהלים וחברים של ערוצי תקשורת בדיוק גבוה מאוד. ההתקפות עובדות על ידי התאמת דפוסי התעבורה של משתמשים שונים לדפוסים של ערוצי תקשורת יעד.
המאמר מציג שתי טכניקות התקפה עיקריות:

1. מתאם מבוסס אירועים - מתאים בין אירועי תקשורת של המשתמש לאלה של הערוץ. אירוע הוא הודעה בודדת או רצף של הודעות.
2. מתאם מבוסס צורה - מתאים בין צורות התעבורה המנומלות של המשתמש ושל הערוץ, כלומר וקטור אורכי החבילות לאורך זמן.

הניסויים הראו שההתקפות עובדות ביעילות רבה נגד Telegram, Signal ו- WhatsApp. למשל, רק 15 דקות של תעבורת טלגרם מאפשרות זיהוי מנהל של ערוץ יעד בדיוק של 94%.
המאמר בוחן גם אמצעי נגד אפשריים כמו הסתרת תעבורה ב-VPN, הוספת תעבורת דמה, ועיכוב חבילות. בנוסף, כותב המאמר מציג מערכת נגד בשם IMProxy שמקשה על ההתקפות.
לסיכום, ההתקפות שמוצגות חושפות פגיעות יסודית ביישומי הודעות מיידיות. הן מצביעות על הצורך של ספקי יישומים אלה ליישם אמצעי הגנה יעילים כדי להגן על משתמשיהם.

<u>תשובות לשאלות:</u>

1. היריב משיג "ground truth" על דפוסי התעבורה של ערוץ היעד ב-IM באחד משלושה האופנים:
- אם זה ערוץ ציבורי פתוח, הוא מצטרף כחבר קריאה בלבד ומקליט מטא-דאטה של ההודעות כמו זמנים וגדלים.
- אם זה ערוץ סגור, הוא מצטרף כמנהל מה שמאפשר לו גם לפרסם הודעות משלו.
- אם זיהה חבר או מנהל, הוא מיירט את התעבורה של אותו משתמש כדי לאפיין את דפוסי הערוץ.

2. היריב מיירט תעבורת רשת על ידי ניטור תעבורת ה-IM המוצפנת של משתמשים. הוא יכול לעשות זאת על ידי מיקום עמדות ציתות ב-ISPs או ב-IXPs שהוא שולט בהם.

3. טבלה 2 מראה סטטיסטיקה של סוגי הודעות שונים שנאספו מערוצי IM אמיתיים. המסקנות העיקריות הן:
- הודעות תמונה הן הנפוצות ביותר, ומהוות 48% מההודעות.
- הודעות וידאו מהוות 95% מנפח התעבורה הכולל בגלל הגודל שלהן.

4. איור 8 מראה איך היריב מוציא אירועי IM ממנות מוצפנות של חבילות. כאשר משתמש שולח/מקבל הודעה, זה יוצר מנה של חבילות קטנות. למרות שאלו מוצפנות, היריב מזהה מנות אלה ומוציא מטא-דאטה על הזמנים, גדלים ותכונות אחרות של אירוע ה-IM.

- <u>הערה :</u> הוספנו לגיט שלנו סיכום יותר מפורט של המאמר (כ-4 עמודים) ובו הסברים יותר מפורטים ומנומקים על כל המאמר.

<u>קישור ל Github שלנו -</u> https://github.com/NoaAmichai/Computer_networks_final_project.git

<u>קישורים לחשבונות הלינקדין :</u> https://www.linkedin.com/in/avi-ostroff-147033257
https://www.linkedin.com/in/noa-amichai-7a65a7190