פרויקט גמר רשתות

מגישים: רועי עופר 208953513
כפיר זילברנגל 209367366

קישור לגיט:
https://github.com/Kfirul/Computers_Network_Final_Project

בגיט מופיעים כל הקבצים, כולל קבצי קוד, תמונות הגרפים, ההקלטות וקבצי ה CSV.
הקובץ הראשי נמצא תחת תיקיית הsrc, קובץ בשם ComputersNetwork.ipynb
מסוג מחברת ג'ופיטר, **הוא מכיל את כל הקוד וכן הסברים מפורטים לגבי כל הליך שביצענו** (הוא מהווה בתור החלק "הרטוב", ומחליף את הPDF)
יש לפעול לפי ההוראות בREADME על מנת שהקובץ ירוץ.

קישור ללינקדאין:

כפיר זילברנגל:
www.linkedin.com/in/kfir-zilbernagel

רועי עופר:
/https://www.linkedin.com/in/ofer-roy-889bb4263

חלק א'(Dry Part):

שם המאמר: Practical Traffic Analysis Attacks on Secure Messaging Applications

אפליקציות מסרים מיידיים מאובטחות כמו טלגרם, סיגנל ו-ווטסאפ הפכו לחלק בלתי נפרד מהחיים שלנו. עם זאת, אפילו אפליקציות מאובטחות ביותר יכולות להיות חשופות להתקפות אם התוקף מכיר את דפוסי התעבורה שלהן.

החוקרים גילו כי כל פעולה המתבצעת באפליקציות אלה - כמו שליחת הודעה, העלאת קובץ או אפילו רק הקלדה - מייצרת זרימת נתוני תקשורת עם דפוסים ייחודיים. על ידי מעקב אחר התעבורה ברשת, ניתן להשתמש במודלים סטטיסטיים כדי לזהות את הדפוסים הללו, ומידע זה ניתן להשתמש כדי לזהות משתמשים ואפילו לפענח את ההודעות שלהם.

הם הצליחו לזהות את כתובות ה-IP של חברי הקבוצה, ואז הם השתמשו במידע זה כדי להאזין לתעבורת הרשת שלהם. על ידי ניתוח זרימת התעבורה, הם הצליחו לזהות את זהות החברים.

ההתקפה של החוקרים היא תזכורת לכך שאפילו אפליקציות מסרים מאובטחות ביותר אינן חסינות לחלוטין מפני התקפות. הנה כמה פרטים נוספים על ההתקפה של החוקרים:

- הם השתמשו במודלים סטטיסטיים כדי לזהות דפוסים בתעבורת הרשת של אפליקציות מסרים מיידיים.
- ההתקפה שלהם היא תזכורת לכך שאפילו אפליקציות מסרים מאובטחות ביותר אינן חסינות לחלוטין מפני התקפות.

התוקף יכול להשיג "אמת יסודית" במספר דרכים אופציונליות כדי להבין את דפוסי זרימת התעבורה של אפליקציות התכתבויות:

1. **קבוצת יעד ציבורית**: אם הקבוצה היעד היא ציבורית (פתוחה לכולם), התוקף יכול להצטרף כחבר רגיל. לאחר הצטרפותו, הוא יכול לצפות בזמן אמת ולהקליט את ההודעות עם נתוני המטא (כמו זמן וגודל ההודעות). דבר זה עשוי לספק תובנות אודות הפעילות של הקבוצה, כמו פעילות גבוהה, כמות החברים, ואפשרי סוגי נושאים.

2. **<u>קבוצת יעד לא ציבורית (אבל התוקף מצליח להצטרף)</u>**: אם התוקף מצליח להצטרף לקבוצה לא ציבורית ויכול לשלוח הודעות, הוא יכול לשלוח הודעות משלו עם דפוסי תעבורה כמו שהם. על ידי ניתוח איך חברים בערוץ מגיבים להודעות אלו, התוקף יכול לקבל מידע נוסף על התנהגות הקבוצה.

3. **<u>קבוצת יעד פרטית (התוקף אינו חבר)</u>**: אם הקבוצה היעד היא פרטית והתוקף לא הצליח להצטרף אליה, אך הוא הצליח לזהות כתובת IP של משתתף/מנהל בקבוצה, הוא יכול להאזין לתעבורת הרשת שלו. דבר זה יאפשר לו לקבוע את דפוסי התעבורה של המשתתף ולספק רמזים אודות הפעילות בערוץ, גם אם התוקף אינו רואה את ההודעות שנשלחות בפועל.

תוקף יכול להאזין לתעבורת הרשת של משתמש על ידי:

- קבלת צו האזנה נסתרת, אם התוקף הוא חברה ממשלתית
- האזנה לתעבורת הרשת של ספק האינטרנט של המשתמש, אשר דרך הנתבים שלו עוברת כל התעבורה.
- האזנה לתעבורת הרשת של IXP, שהוא שרת שמפגיש בין רשתות טלקומוניקציה שונות.

הגודל והתזמון של חבילות רשת יכולים להדליף מידע על זהות השולח או המקבל. לדוגמה, אם שני "אירועים" (הודעות) נשלחים מאותו משתמש ומאותו ערוץ רשת בזמן קצר מאוד, ניתן להניח שהמשתמש השתתף באופן פעיל בערוץ.

ישנם שני אלגוריתמים אפשריים למעקב אחר פעילות רשת:

- אלגוריתם מבוסס אירועים: אלגוריתם זה מזהה אירועים בתעבורת רשת ומשווה אותם לאירועים שנשלחו על ידי משתמש ספציפי. אם יש התאמה רבה בין האירועים, ניתן להניח שהמשתמש השתתף באופן פעיל בערוץ.
- אלגוריתם מבוסס צורה: אלגוריתם זה מחשב את הצורה של התעבורת רשת, שהיא בעצם וקטור של אורכי מנות לאורך זמן. הצורה של התעבורת רשת יכולה לשמש להשוואה ולזיהוי חבילות מאותו סוג שנשלחו והגיעו לכל המשתתפים בערוץ.

הצורה של התעבורת רשת מחושבת על ידי זיהוי "אירועים" בתעבורת הרשת ואז נרמול התעבורה לפי חבילות בגובה שווה. הצורה הסופית מתקבלת מהווקטור שנוצר ממעבר על גבהי האירועים לאורך זמן ההקלטה.

ניתן להשתמש בשני האלגוריתמיים כדי לעקוב אחר פעילות רשת ולהזדהות עם משתמשים שפעילים בערוצים מסוימים. מידע זה יכול לשמש למטרות שונות, כגון מעקב אחר משתמשים, מניעת הונאה או גילוי מתקפות סייבר.

כותבי המאמר רצו לדמות "התקפה" של יריב (למשל ממשלה) על תקשורת רגישה כלשהי (למשל פוליטית). הם עשו זאת על ידי מדידת התעבורה בערוצי רשת ומיינו אותה לפי חמשת סוגי ההודעות הנמצאים בשכיחות הגבוהה ביותר בתעבורה ברשת: קבצים, תמונות, סרטים, אודיו (שמע) והודעות טקסט. להלן טבלה 2 במאמר:

TABLE II: Distribution of various message types

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

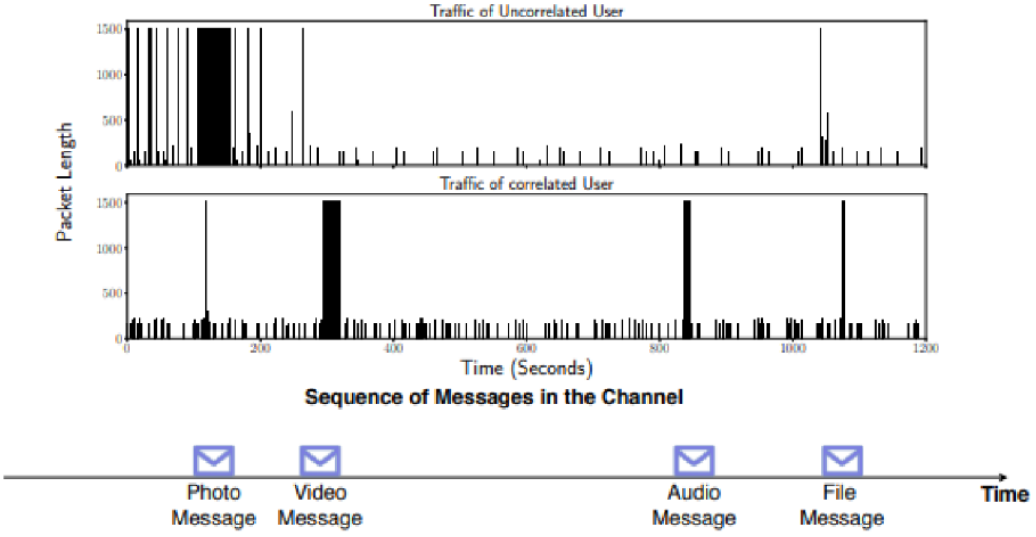
לפי הנתונים שבטבלה, ניתן להסיק מספר דברים:

1. סוג ההודעה הנפוץ ביותר הוא "טקסט" עם 12,539 הודעות, מה שמהווה 29.4% מכל ההודעות בטבלה. זה מראה שרוב ההודעות הם בעלות גודל קטן של כמה בתים.

לעומת זאת, סוג ההודעה הפחות נפוץ הוא "מסמך" עם 903 הודעות, מה שמהווה רק 2.1% מכל ההודעות בטבלה. ניתן לראות שההודעות מסוג זה יחסית נדירות בהשוואה לשאר הסוגים.

2. בהודעות מסוג "וידאו" יש הבחנה ברורה בין גדלי ההודעות. גודל ההודעות משתנה בין 10.16 קילובייט ועד 1.56 גיגהבייט, עם ממוצע של 35.49 מגהבייט. נראה שקיימת מגוון רחב של גדלים להודעות הווידאו, מה שמציין שיכולת האחסון של הסוג הזה משתנה מאוד.

3. ההודעות מסוג "טקסט" ו"תמונה" נמצאות תמיד בגדלים קטנים מאוד. גודל ההודעות מסוג "טקסט" משתנה בין 1 בית ועד 4,095 בתים, עם ממוצע של 306.61 בית. לעומת זאת, גודל ההודעות מסוג "תמונה" משתנה בין 2.4 קילובייט ל-378.68 קילובייט, עם ממוצע של 91.33 קילובייט. ניתן לראות שגם בסוגי ההודעות הללו יש גדלים קטנים, אך עם טווחים מוגבלים יותר.



איור 8 במאמר ממחיש את תהליך חילוץ האירועים מהתנועה של משתמש יעד בהקשר של המתקפה המוצעת. האיור נועד להדגים כיצד ניתן להשתמש בפרצי מנות בתעבורה המוצפנת כדי לזהות ולחלץ אירועי SIM.

האיור מציג ציר זמן לאורך הציר האופקי, המייצג את הזמן שלקח להודעה להשלח. על הציר האנכי את גודל ההודעה.

התעבורה של משתמש היעד מורכבת מחבילות, המיוצגות על ידי מלבנים קטנים. הגודל של כל חבילה אינו מוצג במפורש באיור. החבילות מוצפנות, כך שהתוכן שלהן אינו גלוי ליריב כפי שהוסבר במהלך המאמר.

אירועי ה-SIM הם הודעות ה-IM שנשלחו או התקבלו על ידי משתמש היעד. לפי האיור, ניתן להבחין שאירועי ה-SIM ניתנים להבדלה ויזואלית מהפאקטות הבודדות, מה שמצביע על כך שהם מתרחשים באשכולות או אצווה.

באיור ניתן לראות ש אירועי SIM של תמונות, וידאו, שמע וטקסט (בדגומא באיור 8) מייצרים פרצי מנות, בעוד מנות מפוזרות בגודל קטן מתאימות להודעות פרוטוקול SIM כמו התראות, לחיצות ידיים, עדכונים וכו'. הודעות פרוטוקול אלו קטנות יחסית מהפאקטות הקשורות לאירועי SIM.
כמו כן, באיור ניתן לראות שמבדילים טוב יותר באירועי ה-SIM בתעבורה של משתמש עם קורולוציה לעומת תעבורה של משתמש ללא קורולציה.

כדי לחלץ אירועי SIM, היריב מחפש פרצי מנות בתעבורה. זיהוי התפרצות מתבצע על ידי החלת סף השהייה בין מנות (IPD).

על ידי לכידת פאקטות העומדים בסף ה-IPD, היריב יכול לחלץ אירועי SIM מהתנועה של משתמש היעד. זמן ההגעה של החבילה האחרונה בפרץ נחשב לזמן ההגעה של האירוע, והסכום של כל גדלי החבילות בתוך הפרץ נותן את גודל האירוע.