אוניברסיטת
אריאל
בשומרון

פרויקט גמר רשתות תקשורת:

מגישים: ליאל יואש 206477788,
מאור ברנשטיין 212305965

המאמר אותו חקרנו במהלך הפרוייקט:
[Practical Traffic Analysis Attacks on Secure Messaging Applications]

הרעיון המרכזי של המאמר:

הרעיון המרכזי של המאמר הוא שלמרות מנגנוני ההצפנה המתקדמים המופעלים על ידי יישומי "מסרים מיידיים" (IM- Instant Messaging) מאובטחים פופולריים כמו Telegram, Signal ו-WhatsApp, יישומים אלה עדיין רגישים להתקפות סייבר של ניתוח תעבורת רשת.
מחברי המאמר מראים כי גורמים זרים יכולים לזהות במדויק את כתובות ה-IP של חברים ומנהלים של ערוצי IM ספציפיים על ידי **ניטור** תעבורת הרשת המוצפנת של משתמשי IM פגיעות זו מתעוררת עקב היעדר מנגנוני ערפול תנועה שנפרסו על ידי מפעילי IM, המאפשרים ליריבים לנצל דפוסי תעבורה ולהדליף מידע רגיש גם כאשר ההצפנה קיימת.

מאמר זה מדגיש את האיומים הפוטנציאליים בעולם האמיתי על משתמשים בשירותי IM "מאובטחים" כביכול, במיוחד באזורים שבהם ממשלות מדכאות מנסות לפצח ולהאזין לתושביהם. מחברי המאמר מציגים מודל סטטיסטי למאפייני תעבורת IM, ומפתחים אלגוריתמים המבצע ניתוחי תנועה שיכולים לזהות משתתפים בתקשורת אפליקציות "מסרים מיידים". הם גם דנים באמצעי הגנה אפשריים ומציגים מערכת הגנה אשר נקראת IMProxy.

1. כיצד משיג התוקף מידע ממשי על תעבורת הקבוצה?

עבור כל קבוצה באפליקציית המסרים המיידית(IM) שהוא מטרה , התוקף צריך לאסוף מידע על דפוסי התנועה של המידע בקבוצה. ניתן להשיג זאת באמצעות שלוש שיטות:

ערוצים ציבוריים פתוחים: אם קבוצת היעד הינה ציבורית ופתוחה, התוקף יכול להצטרף כחבר לקבוצה. על ידי הקלטת ההודעות שנשלחו בקבוצה יחד עם הנתונים המרכזיים (Meta Data) שלהן (כגון זמן וגודל הודעה), התוקף יכול לקבל תובנות לגבי תעבורת הקבוצה ואף באילו סוגי נושאים חברי הקבוצה דנים.

פרסום הודעות: אם התוקף חבר בקבוצה ויכול לפרסם בה הודעות, הוא יכול לצפות ישירות בדפוסי התנועה. זה חל על קבוצות סגורות או מצבים שבהם התוקף מקבל הרשאות ניהול בקבוצה. התוקף יכול גם להקליט הודעות קיימות וגם להציג הודעות משלו עם דפוסי תעבורה ברורים.

זיהוי IP של קבוצה פרטית: גם אם התוקף לא יכול להצטרף לקבוצה, אם הוא מגלה את כתובת ה-IP של אחד מחברי הקבוצה או של מנהליה, בצורה זו התוקף יכול להאזין לתנועת הרשת המוצפנת של המשתמש החשוף.
פרצה זו מאפשרת לתוקף לנתח את דפוסי התנועה ולאסוף מידע על פעילות התעבורה בקבוצה.

2. כיצד התוקף מאזין או מצותת לתעבורה ברשת?

ההאזנה של התוקף תתבצע בעזרת ניטור תעבורת הרשת המוצפנת של משתמשי IM. ניתן לנטר זאת על ידי שליטה בנקודות רשת ספציפיות, כגון ספקי שירותי אינטרנט (ISP) או נקודות חילופי אינטרנט (IXPs), שם הן מיירטות את התעבורה. חומת האש הגדולה של סין היא דוגמה למערכת המשמשת ליירוט כזה. לחלופין, התוקף יכול לפקח על תעבורת הרשת של אנשים ספציפיים, פוטנציאלית לאחר שהתוקף השיג צווים משפטיים המאפשרים להאזין למידע בסתר. המטרה היא לנתח את התקשורת המוצפנת שהוחלפה בין משתמשי IM כדי לזהות את המשתתפים בקבוצה או בערוץ היעד ולאתר אותם.

3. תאר בקצרה את המסקנות מטבלה 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

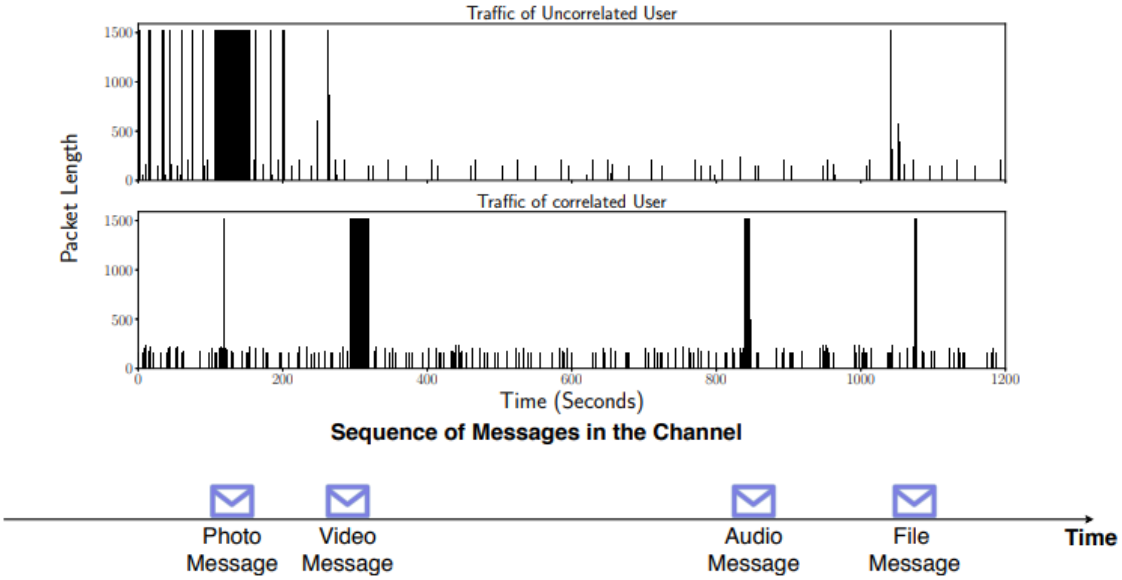
טבלה 2 מספקת פירוט מקיף של סוגי התכנים שהוחלפו ונשלחו באמצעות יישומי הIM, יחד עם נתונים סטטיסטיים רלוונטיים. הטבלה מציגה את התפלגות קטגוריות התוכן, נפח הנתונים הכולל המיוחס לכל קטגוריה, טווח גדלי הקבצים והגודל הממוצע של התוכן בכל קטגוריה.
ניתוח זה מציע תובנות לגבי דינמיקת התוכן ודפוסי צריכת הנתונים בתקשורת IM. הוא מגלה שלסוגים שונים של תוכן, כגון טקסט, תמונות, סרטונים, קבצים ואודיו, יש הפצות, נפחים וגדלים שונים, ומספקים תמונת מצב של מגוון התוכן המשותף בין משתמשי יישום הIM.

התובנות שהבנו מהטבלה:

1. הודעות טקסט מהוות חלק ניכר מההודעות (29.4%), מה שמצביע על כך שתקשורת טקסטואלית היא צורת תקשורת נפוצה.
2. תמונ,u הן הסוג הנפוץ ביותר של הודעות לפי הטבלה, המהוות כמעט מחצית (48%) מההודעות. זה מצביע על כך ששיתוף תמונות הינה דרך פופולרית לתקשורת.
3. הודעות וידאו, למרות שהן חלק קטן יותר (15.4%), שולטות בנפח הכולל (95.3%) בשל גודל הקבצים הגדול יותר שלהן.
4. להודעות טקסט יש גדלים קטנים, עם גודל ממוצע של 306.61 בתים. זה צפוי, מכיוון שהודעות טקסט מורכבות בדרך כלל מפחות נתונים בהשוואה לקובצי מולטימדיה.
5. להודעות תמונה יש גודל ממוצע של 91.33 קילובייט, מה שמצביע על כך שהן מכילות בדרך כלל קבצי תמונה בגודל בינוני כגון בדיחות ומימים.
6. להודעות וידאו יש את טווח הגדלים הגדול ביותר, עם גודל ממוצע של 35.49 מגה בייט. זה משקף את האורך ואיכות הווידאו.
7. להודעות קבצים ואודיו יש גדלים ממוצעים קטנים יחסית לסרטונים, עם 52.56 קילובייט ו-4.44 מגה בייט, בהתאמה.
8. הודעות וידאו תורמות באופן משמעותי לנפח הכולל (95.3%) בשל הגדלים הגדולים שלהן, למרות שהן מהוות חלק קטן יותר מספירת ההודעות (15.4%).
9. הודעות אודיו תופסות 3.92% מהנפח הכולל, מה שמצביע על כך שהן תופסות נפח משמעותי למרות שהן חלק קטן יותר מההודעות.

תובנות אלו יכולות להיות שימושיות להבנת התנהגות המשתמש, ועיצוב אסטרטגיות מיון הנתונים על אף שהם מוצפנים ובכך לחדור לפרטיות המשתמש.

איור 8 מהמאמר: איתור והוצאת מאורעות מהודעות ביישום ה- IM:



איור 8 במאמר ממחיש את תהליך הוצאת האירועים מהודעות ביישום ה IM. באופן ספציפי, הוא מתמקד בהודעות מיידיות שנשלחות או מתקבלות על ידי משתמש יעד. האיור מדגים כיצד נוצרים פרצי פאקטות מוצפנות בהודעות הנל, וכיצד התוקף יכול לאתר מאורעות ספציפיים מפרצי הפאקטות הללו שכן יהיה ניתן לראות זאת גם בפרוייקט שלנו.

המונח "מאורע" מתייחס לפעולה או התרחשות משמעותית, כגון שליחה או קבלה של הודעה, בהקשר של תקשורת מיידית. האיור ממחיש את הרעיון של פרצי פאקטות בצורה ויזואלית, שהן גושים של מידע ברשת כאשר כל הפאקטות מוצפנות ומתאימות למאורעות או הודעות ספציפיים.

תהליך חילוץ המידע כולל זיהוי וקיבוץ פאקטות השייכות לאותה ההודעה. על ידי ניתוח הדפוסים והמאפיינים של פרצי פאקטות אלה, התוקף יכול להסיק מידע על האירועים המתרחשים בתקשורת ה-IM. זה יכול לכלול את תזמון המאורעות(הודעות), המשתתפים המעורבים, ואולי אפילו את התוכן המועבר.

באופן כללי, איור 8 ממחיש את הרעיון של חילוץ הודעות ביישום הIM ומדגיש את תפקידם של פרצי פאקטות בחשיפת תובנות לגבי הפעילויות והאינטראקציות המתרחשות בתקשורת ה-IM.

קישורים:
חשבונות לינקדאין:
Maor Berenstein
Liel Yoash

GitHub Repository:
https://github.com/LielYoash/NetworksFInalProject