יובל בראור 214329633 גוש גורדון 332307073

פרויקט גמר רשתות – חלק יבש:

המאמר "Practical Traffic Analysis Attacks on Secure Messaging Applications" עוסק בפלטפורמות של אפליקציות התכתבויות(IM applications) פופולאריות כגון וואטסאפ, טלגרם וסיגנל המדליפים מידע רגיש על המשתמשים שלהם לתוקפים.
אפליקציות התכתבויות מאובטחות הן חלק בלתי נפרד מהיום יום שלנו, ועל כן אנחנו מצפים כי התקשורת המועברת בה תהייה מאובטחת. התגלה כי אפליקציות אלו לא מאובטחות כמו שחשבנו, וכי התקשורת בהן כפופה למעקב ממשלתי בעיקר עבור התכתבויות בנושאים הרגישים פוליטית וחברתית.

בחלק זה של עבודת הגמר נעסוק בנושא המרכזי של המאמר ונדון בגרפים ושאלות רלוונטיות.

הרעיון המרכזי של המאמר הוא שיח על האבטחה של אפליקציות ההתכתבויות. הם טוענים כי למרות ההצפנה שאפליקציות אלו משתמשות, היא לא מספיקה על מנת להגן על המשתמשים מתוקפים המנסים להגיע למידע.

החוקרים גילו ובנו מודל סטטיסטי המורכב מדאטה שנאסף וסינטטי על מנת לזהות דפוסים של זרימת נתוני תקשורת. דפוסים אלו מתקיימים לאחר כל פעולה שנעשית באפליקציות לדוגמא- העלאת קבצים, הקלדת טקסט ואפילו שליחת הודעה. המודל הסטטיסטי נותן מידע על המשתמשים של האפליקציות, החוקרים קוראים לכך "Traffic Analysis Attack".
בנוסף למודל זה, החוקרים מציגים את אלגוריתמי התקיפות שלהם שמטרתם היא להתאים בין ערוצי התקשורת של האפליקציות האלו לבין המשתמש\מנהל הערוץ באפליקציות אלו.

המחקר ממשיך ומראה כיצד התוקף יכול לקבל אמת קרקעית בנוגע לתעבורה של הערוץ באפליקציה מסוימת:

1. אם הערוץ פתוח, כלומר בהגדרות הגישה הערוף פתוח לכלל הציבור. התוקף יכול להצטרף לערוץ בתור משתמש, לראות את פעילות הערוץ בזמן אמת, להקליט את ההודעות הנשלחות באותו ערוץ מדובר ולקבל את כל הנתונים -meta data (זמן וגודל ההודעות).

2. אם הערוץ פרטי אבל התוקף כן הצליח להיכנס אליה. כאשר הערוץ פרטי, המשתמשים הנמצאים באותו הערוץ יכולים לראות את ההתכתבות בזמן אמת, לשלוח הודעות וכו. בכך, התוקף יכול לבצע ניתוחים סטטיסטיים על המצב בערוץ – התגובות של המשתמשים, נושא השיחה והדפוסים של הקבוצה כולה ובכך להשיג את המידע אותו הוא רוצה.

3. אם הערוץ פרטי והתוקף לא הצליח להיכנס אליה, אבל הוא הצליח לזהות את כתובת ה-IP של אחד המשתמשים, או המנהלים של הערוץ. במקרה זה התוקף יכול לבצע האזנות סתר על הערוץ

המדובר. אותם נתונים שהתוקף יוציא יכולים לשרת אותו למטרותיו (כגון הוצאת הדפוסים של הערוץ, נושא השיחה ועוד).

התוקף מסוגל לבצע האזנת סתר לתנועה ברשת בכמה דרכים:

1. האזנה למשתמשים ספציפיים בעזרת צו להאזנה נסתרת. לדוגמא פעילים חשודים, ממשלות ועוד.
2. האזנה לתנועה ברשת של ספק האינטרנט (ISP).
3. האזנה ל- (internet exchange point) IXP. זוהי נקודה שהשרתים של חברות ה-ISP מתחברות אליהן ולשרתי CDN, ובכך מגבירים את המהירות של הגעת המידע.

כתוצאה מכך התוקף יכול להשתמש באלגוריתם על מנת להתאים בין דפוסי התעבורה של המשתמש עליו הוא מפעיל את ההזנת סתר, לבין האמת הקרקעית של דפוסי ערוץ המבוקש.

התוקף מנסה לקשר זרימות רשת מעורפלות על ידי התאמה בין מאפייני התעבורה שלהן, כלומר תזמוני פאקטות וגדלים של ההודעות. המחקר מגדיש עוד מגוון התקפות ניתוח תנועה אך מתעסק לרוב במה שצוין קודם לכן.

בתרחיש שניתן על ידי המחקר התוקף מיירט זרימת מטרה חיה (למשל, על ידי הצטרפות לערוץ מסוים השנוי במחלוקת בנושא פוליטי), ומנסה להתאים אותו לדפוסי התנועה של זרימות המנותרות בחלקים אחרים של הרשת (כדי להיות מסוגל לזהות את כתובות ה IP-של חברים או מנהלים של ערוץ המבוקש).

לכן, עיצבו אלגוריתמים של מתאם זרימה המותאמים לתרחישים אלו. לשם כך, מדגמים תחילה תנועה ורעש התנהגותי בשירותי האפליקציות, ועל בסיסם מעצבים בהתאמה אישית אלגוריתמים של מתאם זרימה עבור התרחיש הספציפי.

לאחר שימוש בממשק ה API-של Telegram על מנת לאסוף את התקשורת של 1,000 ערוצים אקראיים עם קצבי הודעות שונים, כל אחד עבור טווח של 24 שעות. עבור כל הודעת טלגרם שנאספה, הם חילצו את מזהה הערוץ שאליו נשלח, חותמת הזמן שלו, הסוג של ההודעה (טקסט, תמונה, וידאו, אודיו או קובץ), וגדול ההודעה. נשים לב כי החוקרים השתמשו בהתקפה הדומה ל-Flow Correlation כלומר מציאת קשר בין זרימה ברשת לבין מאפייני התעבורה. ושמו את הנתונים בטבלה בשם TABLE II :

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

הטבלה מציגה את סטטיסטיקת הגודל והתדירות של חמשת סוגי ההודעות העיקריים שנאספו

- טקסט (הודעת טקסט)
- תמונות
- סרטונים
- קבצים
- אודיו

כמו כן ניתן לראות שבעמודה הראשונה מיוצגת המשמעות של חמשת הסוגי ההועדות האלה. בעמודה השנייה ניתן לראות את ההתפלגות של סוגי ההודעות שנאספו במחקר כלומר 29.4% מההודעות היו מסוג טקסט, 48% היו מסוג תמונות, 15.4% היו מסוג סרטונים, 2.1% היו מסוג קבצים ו5.1% היו מסוג אודיו. בעמודה השלישית ניתן לראות גם כן את ההתפלגות ביחס לגודל ההודעות. לא מפתיע שאכן סרטונים , אודיו ותמונות כבדים יותר בדרך כלל מאשר טקסט וקבצים. העמודה הרביעית מציינת את הטווח של גודל המדיה עבור כל סוג.ועמודה החמישית מייצגת את הגודל הממוצע של הודעה מהחמישה סוגים השונים.

החוקרים השתמשו במידע זו על מנת לייצר שרשרת מרקוב ולמדל את התקשורת בערוץ. כתוצאה מכך קיבלנו את מטריצת הסתברות מעבר אמפירית של מודל מרקוב שעוזר בהמשך המחקר .

לאחר המידול, החוקרים מציעים שני אלגוריתמים שבעזרתם ניתן לעקוב אחרי התעבורה של הערוצים: ניתן לשילוב שני האלגוריתמים על מנת לשפר את היכולת לזהות את חברי הקבוצה מתוך תעבורה ולמצוא את האיזון המתאים בין ייעול עלות החישובים לביצועי הזיהוי.

1. ״מזהה מבוסס אירועים- Event based detector״ מתבסס על זיהוי אירועים ספציפיים כמו שליחת הודעה שפורצת את מגבלת הגודל המרבי של פרצים. בעזרת פונקציית קורלציה, ניתן לקבוע האם קשר קיים בין התעבורה של התוקף לבין הקבוצה הנבדקת. ערך הקורלציה מעל ליניארי מסוים מצביע על חברות בין המשתמש והקבוצה.

2. " מבוסס צורה- shape based detector״ מתאים את צורת התעבורה לזיהוי חברי הקבוצה. אמנם האלגוריתם איטי, אך מספק תוצאות מדויקות יותר.

באיור 8 (FIG 8) רואים את התנועה של משתמש עם קורלציה נמוכה ומשתמש עם קורלציה גבוה ביחס לערוץ המבוקש:

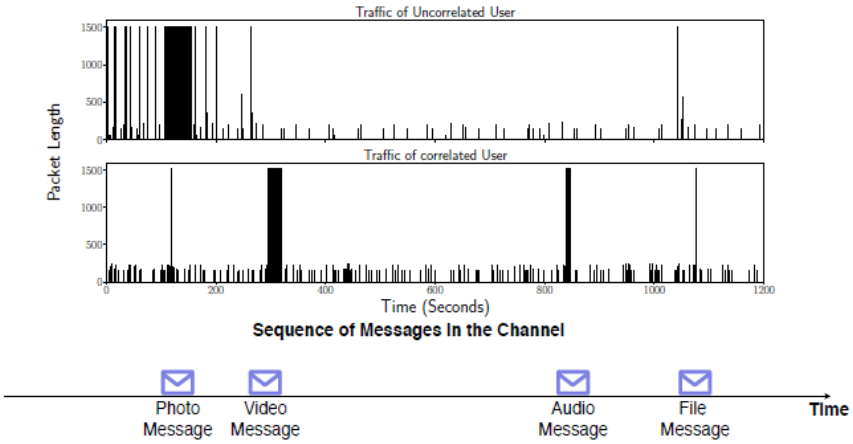

Fig. 8: Event extraction: IM Messages sent/received by a target user create bursts of (encrypted) packets; the adversary can extract events from packet bursts.

ציר ה Y מציין את גודל הפאקטות וציר ה X מציין את הזמן בשניות.
ציר TIME מראה את האמת הקרקעית של שליחת הודעה מסוג תמונה, לאחר מכן הודעה מסוג סרטון ולאחר המתנה קצרה הודעה מסוג אודיו ולסיום שליחת הודעה מסוג קובץ.
ניתן לראות שאכן ציר ה TIME והגרף התחתון יותר תואמים מאשר הגרף העליון ולכן ניתן להגיד שהמשתמש שתנועתו מוצג בגרף התחתון יש יותר קורלציה לערוץ המבוקש (הערוץ שבו שלחו את התמונה, סרטון, אודיו וקובץ).

נשים לב כי בתחתית האיור ניתן לראות אירועים הקורים במהלך פרק הזמן , כאשר עבור המשתמש אשר זוהה כשייך לקבוצה – ניתן לראות שבכל שליחה שכזו יש מספר MTU (maximum transmission unit), בעוד שעבור המשתמש שלא זוהה כשייך לקבוצה ישנם MTU בזמנים שונים, לא בהכרח בזמן אירוע.

ממשיכים להראות את תוצאות המחקר ומגדישים שעשו את זה בצורה מוסרית, בו הם הצטרפו ל500 ערוצי טליגרם מפורסמים באירן והצליחו להתאים בין משתמש חדש שהצטרף לערוץ מסוים לבין הערוץ המסוים. בנוסף, הם מריצים את הניסוי גם על וואטסאפ וסיגנל.

לסיום משווים בין שתי האלגורימים ומראים monte carlo algorithm שתלוי בזמן על מנת לשפר את איכות הדיוק בתוספת 45 דקות (כלומר ב15 דקות בסיס ועוד 45 דקות). בנוסף, מראים איך האלגוריתם פועל שמשתמשים משתמשים ב VPN ודרכים אחרות כדי לשלוח הודעות בערוץ מסוים.

לבסוף החוקרים מציגים מערכת אותה בנו בשם IMProxy. זוהי מערכת נגד התקפות שנוצרה במיוחד לסינון והגנה מפני ניתוחי תעבורה בתכתבויות מיידיות. מערכת זו מוכחת כיעילה ומספקת פתרון מתקדם להתמודדות עם סיכונים והתקפות בתחום זה, תוך שמירה על הפרטיות והאבטחה של המשתמשים.