בס"ד

# פרוייקט גמר קורס

## (רשתות תקשורת)

סמסטר ב תשפ"ג

מגישים :

אילן שמחון ת.ז 212036396

תומר גוזלן ת.ז 314770058

# תוכן העניינים

## הקדמה:

עיקרו של מאמר זה עוסק בחשיפת הסכנות הגלומות בשירותי מסרים מיידיים מאובטחים (IM) בשימוש נרחב למרות השימוש בהצפנה מתקדמת, שירותי IM אלו חשופים לדליפת מידע רגיש לגורמי מעקב.
המאמר מציג התקפות ניתוח תעבורה כאמצעי לפגיעה בפרטיותו של המשתמש בשירותי המסרים.
מחברי המאמר מתמקדים בהתקפות המאפשרות ליריב להבחין בזהות הן של מנהלי מערכת והן של חברים המעורבים בשיחות IM ספציפיות, מבלי תלות ולהסתמך בפרצות תוכנה.

באמצעות חקירה מקיפה של דפוסי תעבורה, המאמר ממחיש כיצד ניתוח תעבורה יכול לחשוף מידע רגיש על תקשורת של משתמשים בשירותי IM. על ידי זיהוי ובדיקה קפדנית של תעבורת רשת מוצפנת, תוקף יכול לחשוף את המשתתפים המעורבים בשיחת IM ממוקדת, ובכך להוות איום משמעותי על פרטיותו של המשתמש.

המשמעות של התקפות אלה משתרעת על תרחישים בעולם האמיתי שבהם מאמצי מעקב וצנזורה נפוצים.
המאמר טוען כי הכרחי עבור שירותי IM לשלב טכניקות ערפול תעבורה כדי לנטרל את הסכנות המנוצלות על ידי התקפות ניתוח תעבורה.

יתרה מכך, המחברים פיתחו מערכת חדשנית למניעת התקפות בשם IMProxy.
בנוסף, המאמר שופך אור על המודלים הסטטיסטיים העקרונות, שיטות הפעולה, החוקים וההנחות של איסוף הנתונים המשמשות לבדיקת דפוסי תעבורת IM, מה שמספק בסיס איתן לאלגוריתמי ההתקפה שלהם.

במהותו, מאמר זה משמש כקריאת השכמה, המאיר את סיכוני הפרטיות הנלווים בשימוש בשירותי IM מאובטחים פופולריים. הוא מדגיש את הצורך באמצעי אבטחה משופרים לשמירה על פרטיות המשתמש בעידן המסומן בנוכחות הולכת וגוברת של מאמצי מעקב וצנזורה.

# שאלה מספר 1

How does the attacker obtтain ground truth about the traffic of the channel ?

---

בהקשר של שירותי מסרים מיידיים (IM), מאמר זה מתעמק בתהליך של גילוי וניצול הסכנות הקיימות בפלטפורמות מאובטחות ומוצפנות המהוות בטן רכה לדליפת מידע רגיש לגורמי מעקב.
התוקף משתמש בעקרונות, שיטות הפעולה, חוקים והנחות שונות כדי לחשוף ולנצל חולשות אלו, במיוחד ביחס לדפוסי התעבורה בתוך שירותי IM.
המטרה העיקרית של התוקף היא להשיג מידע מדויק ואמין (Ground truth) לגבי התעבורה של ערוץ היעד.
הדבר כרוך בחקירה מעמיקה של גישות שונות המאפשרות לתוקף לאסוף מידע רב ערך ולבצע ניתוח מקיף של לתבניות התקשורת בתוך שירות ה-IM.

<u>הצטרפות לערוץ פתוח (ציבורי)</u>

אחת משיטות המפתח שבהן משתמש התוקף היא הצטרפות לערוץ פתוח (ציבורי) בתוך שירות ה-IM.
על ידי הפיכתו לחבר בערוץ, התוקף מקבל את היכולת להשתתף באופן פעיל בתקשורת השוטפת. מעורבות ישירה זו מספקת הבנה ממקור ראשון של ההודעות שהוחלפו בתוך הערוץ, הכולל את המטא-נתונים (Metadata) הקשורים אליהם, כמו חותמות זמן וגדלים של הודעות. על ידי התבוננות ורישום של פעילויות התקשורת, התוקף מקבל תובנות חשובות לגבי הדפוסים והדינמיקה של תעבורת הערוץ.

<u>הרשאות גישה\ניהול בתוך הערוץ</u>

במצבים בהם ערוץ היעד אינו פתוח לגישה ציבורית, התוקף עשוי לבקש לרכוש חברות או הרשאות ניהול בתוך הערוץ. ניתן להשיג זאת באמצעים שונים, כמו להיות חבר בקבוצה סגורה המאפשרת פרסום הודעות או השגת תפקיד ניהולי בקבוצה. ברגע שהרשאות אלו מתקבלות, התוקף מקבל את היכולת לתרום באופן פעיל הודעות לערוץ ולנתח את דפוסי התנועה המובהקים הקשורים לסוגי הודעות שונים או למשתמשים ספציפיים.
באמצעות תהליך זה של האזנה מספקת לתוקף הבנה מעמיקה יותר של דינמיקת התקשורת בתוך הערוץ, ומאפשרת לו לאסוף מידע חיוני על התנהגות התנועה והדפוסים בתוך הערוץ.

<u>ציתות לבעלי גישה ע"י זיהוי כתובת IP</u>

במקרים בהם השתתפות ישירה או גישה מנהלתית מתבררת כבלתי ניתנת להשגה, התוקף עשוי לפנות לצותת לחבר או מנהל של ערוץ יעד התקיפה. זה כרוך בזיהוי כתובת ה-IP של חבר או מנהל ספציפי ובביצוע האזנה מקוונת אחר תעבורת הרשת שלהם. באמצעות תהליך זה של האזנה, התוקף יכול לאסוף מידע מוצק על התנהגות התנועה והנתונים המשקפים את ערוץ התקשורת. ניתוח דפוסי התעבורה של החבר או המנהל מאפשר לתוקף להסיק תובנות לגבי התקשורת הכוללת בתוך הערוץ.

שימוש בגישות אלו מאפשרות לתוקף לרכוש מידע מדויק ואמין על תעבורת הערוץ.
המידע שנרכש משמש בסיס לניתוח ולפיתוח של אלגוריתמים מתוחכמים להתקפות ניתוח תעבורה.
עם הבנה מקיפה על התנהגות התקשורת, סוגי ההודעות, הגדלים והעיכובים בין הודעות, התוקף יכול לתכנן אסטרטגיות יעילות לזיהוי משתתפים, מנהלי מערכת או תוכן רגיש בשירות ה-IM.

לסיכום, מאמר זה מספק תובנות חשובות לגבי התהליך המדוקדק שמפעיל תוקף כדי להשיג ראיות מוצקות לגבי דפוסי התעבורה בשירותי מסרים מיידיים. על ידי שימוש בגישות שונות כגון השתתפות ישירה, הרשאת גישה מנהלתית והאזנת סתר, התוקף רוכש בהצלחה מידע חיוני המשמש כבסיס לניתוח נתונים שלאחר מכן יפותחו אלגוריתמים מתוחכמים להתקפות ניתוח תעבורה. המאמר שופך אור על נקודות התורפה הגלומות בשירותי IM, ומדגיש את הצורך באמצעי אבטחה חזקים כדי לשמור על פרטיות המשתמש ולהבטיח את סודיות התקשורת.

# שאלה מספר 2

How does the attacker wiretap the network traffic ?

---

בתחום שירותי ההודעות המיידיות (IM), תעבורת האזנות סתר משמשת אמצעי רב עוצמה לתוקפים לקבל גישה למידע רגיש ולבצע התקפות ניתוח תעבורה. שיטה זו כוללת האזה לתעבורת הרשת המוצפנת של משתמשי IM.תהליך האזנת סתר לתעבורת רשת מתחיל בכך שהתוקף מזהה את ערוץ ה-IM היעד או משתמשים ספציפיים שאחר התעבורה שלהם מעוניינים לעקוב. לתוקף עשוי להיות ידע מוקדם מה שגורם להם למקד את מאמציהם לציתות לערוצי התקשורת.
לאחר זיהוי המטרה, התוקף מגדיר מנגנון מעקב אחר תעבורת הרשת של משתמשי ה-IM שנבחרו. האזנה זו זה יכול להתרחש בנקודות שונות במסלול התקשורת, בהתאם לרמת הגישה שיש לתוקף או הכלים והמשאבים העומדים לרשותו.

<u>האזנת סתר לתעבורת רשת באמצעות ISP ו-IXPs</u>

גישה נפוצה אחת להאזנת סתר לתעבורת רשת כוללת השגת שליטה על ספקי שירותי אינטרנט (ISP) או נקודות חילופי אינטרנט (IXPs). על ידי פגיעה במרכיבי תשתית הרשת החיוניים הללו, התוקף יכול לקבל גישה לחבילות הנתונים הזורמות ברשת. זה מאפשר להם לצפות ולנתח אחר זרימת התקשורת המוצפנת של משתמשי ה-IM.

<u>מיקוד האזנת סתר לתעבורת רשת לאנשים מסויימים</u>

במקביל, התוקף עשוי להתמקד באנשים מסויימים שהם חושדים שהם מעורבים בערוץ ה-IM של המטרה או בתקשורת עצמה. בתרחיש זה, התוקף עלול לקבל צו האזנת סתר, המעניק לו סמכות חוקית לצותת אחר תעבורת הרשת של אנשים אלו. גישה זו מופעלת לרוב על ידי רשויות אכיפת החוק בחקירות הכרוכות בחשד לפעילות פלילית.

ברגע שתעבורת הרשת במעקב, התוקף ממשיך בניתוח הנתונים. ניתוח זה כולל פענוח של תוכן התקשורת המוצפן כדי לחשוף את ההודעות המוחלפות בין משתמשי ה-IM. התוקף עשוי להשתמש בטכניקות ובכלים שונים כדי לפענח את הנתונים, בהתאם לפרוטוקולי ההצפנה המופעלים על ידי שירות ה-IM.

לבסוף,האזנת סתר לתעבורה ברשת משמשת כלי רב עוצמה לקבל גישה למידע רגיש ולבצע התקפות בתחום שירותי המסרים המיידיים. על ידי מעקב וניתוח תעבורת רשת מוצפנת, התוקפים יכולים לקבל ראיות מוצקות מכריעות לגבי התנהגות התקשורת בשירות ה-IM. עם זאת, חשוב לציין כי האזנת סתר היא פעילות רגישה ביותר ושנויה במחלוקת משפטית המעוררת דאגות רציניות בנוגע לפרטיות. לדברי מחברי המאמר שירותי המסרים חייבים ליישם הצפנה חזקה מקצה לקצה כדי להגן על פרטיות המשתמש ולהגן מפני התקפות כאלה.

# שאלה מספר 3

Describe shortly the conclusions from Table II in the paper ?

---

טבלה II במאמר מציגה ניתוח מקיף של התפלגות סוגי הודעות שונים בנתוני תעבורת ה-IM שנאספו מאפליקציית טלגרם. הטבלה מספקת תובנות חיוניות לגבי ההרכב, הנפח והמאפיינים של סוגי הודעות שונים המוחלפים בשירות ה-IM. נבחין במסקנות בניתן להסיק מטבלה II.

<u>שכיחות סוג הודעה:</u>

הנתונים המוצגים בטבלה מדגישים את השכיחות של סוגי הודעות שונים בתקשורת ה-IM. מבין ההודעות המנותחות מופיעות הודעות התמונה כשכיחות ביותר, המהוות 48% מסך ההודעות שנאספו מערוצי הטלגרם. הודעות טקסט הן השניות בשכיחותן, המהוות 29.4% מסך ההודעות.הודעות וידאו, שלרוב גדולות יותר בגודלן,הן כסוג ההודעות השלישי בשכיחותו מייצגות 15.4% מההודעות.
להודעות קבצים ולהודעות שמע יש תדרים נמוכים יחסית.

<u>התפלגות נפח הנתונים:</u>

הנפח מתייחס לכמות הנתונים הכוללת שמועברת בשירותי המסרים (IM) בסוג הודעה ספציפי.
התפלגות נפח הנתונים על פני סוגי מסרים שונים חושפת ממצא מפתיע. הודעות וידאו שולטות בתעבורת ה-IM במונחים של נפח נתונים, ותורמות ל-95.3% מהנפח הכולל. ממצאים אלה מצביעים על כך שהודעות וידאו, אף שהן סוג ההודעות השלישי בשכיחותו, תורמות באופן משמעותי לכלל הנתונים המוחלפים בשירות ה-IM.התפלגות משמעותית זו יכולה להצביע על הפופולריות הגבוהה בקרב שליחת הודעות וידאו בטלגרם.
בנוסף הוא כי הודעות שמע תורמות ל-3.92% מנפח הנתונים, בעוד שהודעות תמונה מהוות 0.765% מהנפח הכולל. הודעות טקסט והודעות קבצים מייצגות פרופורציות נמוכות מנפח הנתונים הכולל.

<u>התפלגות גודל ההודעה:</u>

טווח הגדלים של כל סוג הודעה משתנה באופן משמעותי, המשקף את הגיוון באופי התקשורת בתוך שירות ה-IM.ניתן להבחין כי הודעות מסוג הוידאו והקבצים גוברות על יתר סוגי ההודעות במונחי טווחי הגודל המועברים.הודעות הווידאו מציגות את טווח הגדלים הרחב ביותר, החל מ-10.16 (KB) ועד ל-1.56 (GB), עם גודל ממוצע של 35.49 (MB). הודעות קבצים, שיכולות לכלול מגוון קבצים מצורפים, נעות בין 2.54 (KB) ל-1.88 (MB), בגודל ממוצע של 52.56 (KB).הגודל הממוצע של הודעות מתיישב עם נפח הנתונים שלהן, כאשר הודעות הווידאו הן הגדולות ביותר והודעות הטקסט הן הקטנות ביותר בממוצע.

ממצאים אלו שופכים אור על דינמיקת האינטראקציות בין המשתמשים בתוך פלטפורמת ה-IM (טלגרם). השכיחות של הודעות תמונה ווידאו מעידה על החשיבות ההולכת וגוברת של תכני מולטימדיה בתקשורת, בעוד שהדומיננטיות של הודעות וידאו מבחינת נפח הנתונים מדגישה את הצורך במנגנוני טיפול והעברת נתונים באופן יעיל בשירותי IM.טבלה זו מספקת נתונים קריטיים המאפשרים לנו לקבל הבנה מעמיקה יותר של המאפיינים של תעבורת התקשורת.

# שאלה מספר 4

Fig. 8 in the paper

---

איור 8 במאמר מייצג חזותית את תהליך חילוץ האירועים מתעבורת התקשורת המוצפנת של משתמש יעד כלשהו ,כחלק מהתקפות ניתוח התעבורה לשירותי הודעות מיידיות מאובטחות (SIM).
המטרה העיקרית של איור זה היא להציג כיצד היריב יכול לזהות ולחלץ אירועי SIM, כגון הודעות שנשלחו מתעבורת משתמש היעד בהתבסס על דפוסי התפרצות שנצפו בחבילות המוצפנות.

ציר ה-x של הגרף מייצג את ההשהיות בין ההודעות בשניות, בעוד שציר ה-y מציג את אורך המנות בתעבורה ( Packet Lengt) האיור מציג שני גרפים נפרדים המבחינים בין התעבורה של שני משתמשים: משתמש אחד עם תעבורה לא מתואמת (Traffic of Uncorrelated User) והמשתמש השני עם מתאם (Traffic of User Correlated).ניתן להבחין כי התעבורה של משתמש היעד מורכבת מחבילות, המיוצגות על ידי מלבנים קטנים.

האיור מדגים כיצד אירועי SIM, כגון שליחת תמונה או הודעה, מובילים לפרץ של מנות בתעבורה המוצפנת. התפרצויות אלה מורכבות מחבילות עם עיכובים קטנים מאוד בין-מנות.
לא ניתן לפענח ישירות את החבילות המוצפנות בתוך התפרצויות אלה עקב הצפנה, אך תבנית ההתפרצות הייחודית שלהן יכולה להיות מזוהה על ידי התוקף.הניתוח הוויזואלי מצביע על ההבדל הברור בצורת התעבורה של אירועי ה-SIM בתעבורת משתמש היעד.
התוקף משווה את המרווחים בין חבילות הנתונים ומזהה קבוצות שביניהן המרווחים קטנים מתוך התעבורה המוצפנת. תהליך זה מאפשר לו לזהות אירועים ספציפיים ולמצוא אותם בתוך התעבורה הקיימת, ובכך להבחין בפרצי מנות. בנוסף , התוקף מבצע סינון של המלבנים הקטנים והנפרדים מתוך התעבורה.
המלבנים הללו מייצגים את המסרים הנוספים בתוך התעבורה של משתמש היעד, כגון הודעות מתוך פרוטוקול ה-SIM, הודעות ידועות, ועדכונים.

לסיכום, האיור מציג תהליך שבו התוקף יכול לזהות ולחלץ אירועי SIM בתוך תעבורה מוצפנת, והדגמה של דפוס התפרצויות הייחודי של ה-SIM עם המרווחים הקטנים ביניהן, ואיך הם נראים בשונים מהתעבורה של משתמש ללא קורולציה. תהליך זה מהווה חלק מהתקפות ניתוח התעבורה, והוא מספק דרך חזקה ויעילה לזהות אירועי SIM במערכות המאובטחות.

# נספח א׳

Table Ⅱ : Distribution of various message types

---

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 |

## נספח ב׳

Fig. 8: 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.

---