***Network Project***

פתיחה

המאמר, "Practical Traffic Analysis Attacks on Secure Messaging Applications", נכתב על ידי אלירזה בהרמאלי, אמיר הומאנסאדר, רמין סולטני, דניס גוקל ודון טאוסלי מאמהרסט, מאוניברסיטת מסצ'וסטס אמהרסט. החוקרים בדקו כיצד ניתן להתקיף אפליקציות מאובטחות ופופולריות המיועדות להתכתבויות (IM=instant messaging) בהקשרים של מעקב וצנזורה. הרקע לכתיבת המאמר הוא העידן הנוכחי, בו אפליקציות התכתבויות מאובטחות כמו טלגרם, סיגנל ווואטסאפ הפכו לחלק בלתי נפרד מהתקשורת היומיומית. פלטפורמות אלו, על אף שהן מספקות מרחב לתקשורת מיידית ומאובטחת (מבחינת תוכן ההתכתבויות), כפופות לסיכונים הנובעים ממעקב וצנזורה ממשלתיים. סיכונים אלו רלוונטיים במיוחד כאשר הפלטפורמות הללו משמשות מרחב להתכתבויות בנושאים רגישים חברתית ופוליטית.

**הרעיון המרכזי**

הרעיון המרכזי של המאמר הוא העלאת מודעות לגבי האבטחה של האפליקציות המדוברות.   
החוקרים מסבירים שאפילו הצפנה מתקדמת, המופעלת על ידי אפליקציות שונות, עשויה שלא להספיק כדי להגן באופן מלא על מידע משתמש רגיש מפני יריבים עם הכלים והטכניקות הנכונות – כאשר יריב מתואר כארגון מעקב (כממשלה או ארגון המשויך אליה) אשר מטרתו לזהות (על ידי זיהוי כתובות IP) של חברים או מנהלים של קבוצת התכתבויות מסוימת (כפי שצוין קודם לכן, מקור מטרה זו יכול להיות רצון למעקב אחרי מתנגדי משטר, צנזורת תכנים מסוימים וכדומה, כפי שניתן דוגמא במאמר לגבי איראן, רוסיה וסין).

על אף העובדה שתוכן התקשורת מוצפן בצורה מאובטחת באפליקציות הנ"ל, החוקרים הדגימו כי על ידי מעקב אחר התעבורה ברשת ניתן על ידי מודלים סטטיסטים לזהות דפוסים של זרימת התעבורה, שעל ידיהם הם יכולים לספק שפע של מידע, שהמשתמש ומפעיל הIM היו שמחים שלא יהיו חשופים ליריב/ תוקף. החוקרים גילו כי כל פעולה שמתבצעת בתוך יישומים אלה - כמו שליחת הודעה, העלאת קובץ או אפילו רק הקלדה - מייצרת זרימת נתוני תקשורת עם דפוסים ייחודיים. אם כן התוקף, על ידי ניטור וניתוח של דפוסים אלה בלבד, יכול לאסוף מידע רב ערך על משתמשים ופעילויותיהם. החוקרים מגדירים זאת כ’Traffic Analysis Attack’.

***שאלה 1:***

התוקף משיג יכול להשיג אמת קרקע בכמה דרכים:

1. אם הערוץ ציבורי כלומר פתוח היריב פשוט מצטרף לערוץ ומתעד את ההודעות הנשלחות בערוץ הנ"ל יחד עם המטא נתונים שלהם כמו (גודל , זמן, דילאי, וכו,)
2. היריב מצטרף לערוץ והוא יכול לפרסם הודעות בערוץ הנ"ל, זה יכול להתרחש אם הערוץ סגור שנותן לכל חבר את היכולת לפרסם הודעות או שזה יכול להיות ערוץ בו רק המנהל יכול לפרסם הודעות והיריב קיבל תפקיד מנהל.

במקרה זה היריב יכול לא רק לתעד הודעות שפורסמו בערוץ אלא גם לפרסם הוא בעצמו הודעות לערוץ זה עם דפוסי התנועה הרצויים.

1. הערוץ הינו פרטי והיריב אינו יכול להצטרף לערוץ אבל הוא זיהה את הפרטים של חבר/ מנהל בערוץ. היריב מאזין לתעבורת הרשת המוצפנת של החבר בערוץ שזיהנו ומתעד את דפוסי התנועה שלו.

***שאלה 2:***

היריב מפקח על תעבורת הרשת המוצפנת של משתמשי IM על מנת לזהות את המשתמשים/מנהלים של ערוץ IM שמסומן כיעד.

ניתן לבצע זאת על ידי האזנת סתר של היריב לתעבורת הרשת של ספקי האינטרנט או נקודות הביניים בה מתחלפת התעבורה שלהם לדוגמה חומת ההגנה של האינטרנט בסין.

לחלופין, היריב יכול להאזין לתעבורת הרשת של אנשים ספציפיים(למשל חשודים) אולי לאחר קבלת צו האזנת סתר.

***שאלה 3:***

אנו יודעים כי שירותי IM מאפשרות שליחה של 5 סוגי הודעות (Text, Video, Audio, File, Photo) ובטלה II נשים לב כי מוצג המידע הסטטיסטי של ההודעות שנשלחו בערוץ זה לפי סוג ההודעות והמאפיינים של כל הודעה שהם כמות ההודעות מאותו סוג, נפח ההודעה (גודל ההודעה), טווח הגודל בו נמצאת כל סוג הודעה, גודל ממוצע של כל סוג.

הדרך בה החוקרים מנחתים את התעבורה היא בכך שהם מעריכים את נפחם וגודלם של הפאקטות הנשלחות וזמן התעבורה בין שני הצדדים.

מטבלה II אני מסיקים כי רוב ההודעות המועברות בקבוצה הן תמונות שמהוות כ48% מהתעבורה לאחר מכן הודעות טקסט שמהוות כ-29.4% מהתעבורה, ווידאו שמהווה כ- 15.4% , שמע שמהווה כ- 5.1% ולאחר מכן קבצים שמהווים 2.1% מכלל התעבורה.

***שאלה 4:***

בתרחיש רשת הכולל תעבורה מוצפנת, אירועים מסוימים (כמו שליחת תמונה) מובילים ליצירת פרצי מנות. התפרצויות אלו מורכבות מחבילות בגדלים התואמים את גודל יחידת השידור המקסימלית (MTU). התזמון בין החבילות הללו קצר מאוד. ישנן גם מנות מפוזרות בגודל קטן יותר בתוך התפרצויות אלה, המייצגות הודעות פרוטוקול SIM כגון התראות, לחיצות ידיים ועדכונים.

למרות ההצפנה, צופה (יריב) יכול להסיק אירועים אלו על ידי זיהוי התפרצויות אלו של מנות בגודל MTU. הם משתמשים בפרמטר שנקרא "סף "IPD (te) כדי להבחין בין התפרצויות. אם הפרש הזמן בין שתי מנות קטן מ-te)), מנות אלו נחשבות לחלק מאותו פרץ.

עבור כל פרץ, היריב מפרש אותו כאירוע SIM. זמן ההגעה של החבילה האחרונה בפרץ מציין

מתי התרחש האירוע, והגודל הכולל של החבילות בפרץ משקף את גודל האירוע. אם שתי

הודעות SIM נשלחות בהפרש זמן קטן מ-te, הן יטופלו כאירוע בודד.

כמו כן, היריב משלב אירועים קרובים יותר ממך כאשר הם נצפים בערוץ היעד.

למעשה, שיטה זו מאפשרת למתבונן לזהות אירועים (כמו שליחת תמונות) בתעבורה מוצפנת על ידי זיהוי דפוסים של התפרצויות מתוזמנות מקרוב של מנות בגודל MTU, למרות שתוכן החבילות נשאר מוצפן. לפרמטר te יש תפקיד מכריע בהגדרת התפרצויות אלו.

לכן Fig.8 ניתן לראות כי קיימים שני איורים המייצגים שני מאורעות:

באיור העליון מיוצג גרף האזנה שבגרף מתרחש מאורע בו אין התאמה בין פרצי הפאקטות (MTUsize) שנשלחו בחבילה לבין פרצי הפאקטות המאפיינות את סוגי ההודעות שהציגו החוקרים.

האיור התחתון מיוצג גרף האזנה שבו יש התאמה בין פרצי הפאקטות שהתקבלו לבין פרצי הפאקטות המאפיינות את סוגי ההודעות שהציגו החוקרים, לכן רואים את סוגי ההודעות שמתאים לאותו מאורע.

The article "Practical Traffic Analysis Attacks on Secure Messaging Applications" was authored by Elirazha Baharmali, Amir Hoomansadar, Ramin Soltani, Denis Guckel, and Don Towsley from the University of Massachusetts Amherst. The researchers examined how secure and popular instant messaging (IM) applications can be vulnerable to attacks in contexts involving surveillance and censorship. The backdrop for the article's creation lies in the current era, where secure IM applications such as Telegram, Signal, and WhatsApp have become integral parts of daily communication. While these platforms offer a space for immediate and secure communication (in terms of message content), they are susceptible to risks arising from governmental surveillance and censorship. These risks are particularly relevant when these platforms are used for sensitive social and political conversations.

The paper titled "Exploring Practical Traffic Analysis Attacks on Secure Messaging Applications" was authored by Elirazha Baharmali, Amir Hoomansadar, Ramin Soltani, Denis Guckel, and Don Towsley, all associated with the University of Massachusetts Amherst. The researchers delved into the potential vulnerabilities of well-regarded secure instant messaging (IM) applications, particularly in scenarios involving surveillance and censorship. The genesis of this study is rooted in the contemporary landscape, where widely-used IM platforms like Telegram, Signal, and WhatsApp have seamlessly integrated into our daily communication routines. Despite offering a haven for prompt and confidential exchanges, these platforms are not immune to risks stemming from governmental monitoring and content control. These challenges become especially pertinent when these platforms are utilized for discussions encompassing sensitive societal and political topics.

המאמר "התקפות מעשי ניתוח תנועה על יישומי הודעות מאובטחות" נכתב על ידי אלירזה בהארמלי, אמיר הומנסאדר, רמין סולטני, דניס גוקל ודון טאוסלי מאוניברסיטת מסצ'וסטס אמהרסט. החוקרים בדקו כיצד יישומי מסרים מיידיים (IM) מאובטחים ופופולריים יכולים להיות פגיעים להתקפות בהקשרים הכוללים מעקב וצנזורה. הרקע ליצירת המאמר טמון בעידן הנוכחי, בו אפליקציות IM מאובטחות כמו Telegram, Signal ו-WhatsApp הפכו לחלק בלתי נפרד מהתקשורת היומיומית. בעוד שפלטפורמות אלו מציעות מרחב לתקשורת מיידית ומאובטחת (מבחינת תוכן ההודעות), הן חשופות לסיכונים הנובעים ממעקב וצנזורה ממשלתית. סיכונים אלו רלוונטיים במיוחד כאשר פלטפורמות אלו משמשות לשיחות חברתיות ופוליטיות רגישות.

המאמר שכותרתו "חקירת התקפות מעשיות של ניתוח תנועה על יישומי הודעות מאובטחות" נכתב על ידי אלירזה בהארמלי, אמיר הומנסאדר, רמין סולטני, דניס גוקל ודון טאוסלי, כולם קשורים לאוניברסיטת מסצ'וסטס אמהרסט. החוקרים התעמקו בפגיעויות הפוטנציאליות של יישומי הודעות מיידיות מאובטחות (IM) נחשבות, במיוחד בתרחישים הכוללים מעקב וצנזורה. ראשיתו של מחקר זה מושרשת בנוף העכשווי, שבו פלטפורמות IM בשימוש נרחב כמו Telegram, Signal ו-WhatsApp השתלבו בצורה חלקה בשגרת התקשורת היומיומית שלנו. למרות שהן מציעות מקלט לחילופי דברים מיידיים וחסויים, פלטפורמות אלו אינן חסינות מפני סיכונים הנובעים מפיקוח ממשלתי ובקרת תוכן. אתגרים אלו הופכים רלוונטיים במיוחד כאשר פלטפורמות אלו משמשות לדיונים הכוללים נושאים חברתיים ופוליטיים רגישים.

The central idea of the article is to raise awareness about the security of the mentioned applications. The researchers explain that even advanced encryption implemented by various apps might not fully safeguard sensitive user information from adversaries with the right tools and techniques. Here, an adversary is depicted as a surveillance entity (such as a government or an affiliated organization) aiming to identify (by IP address identification) members or administrators of a specific messaging group. This goal could be driven by motives like tracking dissenters, content censorship, and more, as exemplified in the article concerning Iran, Russia, and China.

Despite the secure encryption of communication content in these applications, the researchers demonstrate that by monitoring network traffic, statistical models can identify patterns of traffic flow. These patterns can provide a wealth of information, potentially revealing user and IM operator behaviors without them being exposed to adversaries or attackers. The researchers discovered that every action within these apps - be it sending a message, uploading a file, or even just typing - generates a unique communication data flow pattern. Hence, an attacker, through monitoring and analyzing these patterns alone, can gather valuable information about users and their activities. The researchers term this phenomenon a "Traffic Analysis Attack."

The core concept of the article aims to raise awareness regarding the security landscape of the mentioned applications. The researchers elucidate that despite the incorporation of sophisticated encryption techniques by various apps, they may not provide comprehensive protection for sensitive user data against adversaries equipped with appropriate tools and methodologies. Here, an adversary is portrayed as a surveillance entity, such as a government or an affiliated group, with the intention of identifying members or administrators of a specific messaging group through IP address tracing. This objective might stem from motives like monitoring dissent, enforcing content censorship, and more, as illustrated in the article's context involving Iran, Russia, and China.

Even though these applications ensure robust encryption for communication content, the researchers demonstrate that monitoring network traffic enables statistical models to discern patterns in the flow of data. These patterns can yield a treasure trove of insights, potentially exposing user behaviors and activities of instant messaging operators without their knowledge. The researchers unearthed that each action undertaken within these apps - whether it's sending a message, uploading a file, or simply typing - generates a distinct pattern in communication data flow. Consequently, an attacker can glean valuable information about users and their engagements solely by scrutinizing and interpreting these patterns. The researchers coin this phenomenon as a "Traffic Analysis Attack."

Top of Form

ChatGPT

הרעיון המרכזי של המאמר הוא להגביר את המודעות לנוגע לנוף האבטחה של האפליקציות שהוזכרו. החוקרים מבהירים כי למרות השימוש בטכניקות הצפנה מתקדמות באפליקציות שונות, יתכן כי לא יוענק הגנה מקיפה למידע רגיש של המשתמשים מפני יריבים שזוכים בכלי וטכניקות המתאימים. כאן, יריב נמצא בתפקיד של ארגון מעקב כמו ממשלה או קבוצה משוייכת, ומטרתו לזהות חברים או מנהלי קבוצת התכתבויות מסוימת באמצעות מעקב אחר כתובות ה-IP. מטרה זו עשויה להצאת נגזרות מרקעים כמו מעקב אחר התנגדות, צנזורת תוכן, ועוד, כפי שנמצא בהקשר המוצג במאמר על איראן, רוסיה וסין.

למרות שאלו האפליקציות מבטיחות הצפנה מאובטחת עבור תוכן התקשורת, החוקרים מדגימים כי בעזרת מעקב אחר תעבורה ברשת, ניתן להשתמש במודלים סטטיסטיים לזיהוי דפוסים של זרימת הנתונים. הדפוסים אלו יכולים לספק מקור עשיר לתובנות, ובכך לחשוף פעולות של משתמשים ומפעילי התכתבויות בלתי נראית ליריבים או לתוקפים. החוקרים גילו כי כל פעולה באפליקציות אלו - בין שמדובר בשליחת הודעה, העלאת קובץ, או פשוט הקלדה - מייצרת דפוס ייחודי בזרימת הנתונים בתקשורת. לכן, תוקף יכול להשיג מידע יקר על משתמשים ופעילויותיהם בלבד על ידי ניטור ופיענוח של הדפוסים הללו. החוקרים מקראים לתופעה זו "התקפת ניתוח תעבורה" ("Traffic Analysis Attack").

Google translate:

תפיסת הליבה של המאמר נועדה להעלות את המודעות לגבי נוף האבטחה של האפליקציות המוזכרות. החוקרים מבהירים שלמרות השילוב של טכניקות הצפנה מתוחכמות על ידי אפליקציות שונות, ייתכן שהם לא יספקו הגנה מקיפה לנתוני משתמשים רגישים מפני יריבים המצוידים בכלים ומתודולוגיות מתאימות. כאן, יריב מוצג כישות מעקב, כגון ממשלה או קבוצה קשורה, מתוך כוונה לזהות חברים או מנהלים של קבוצת הודעות ספציפית באמצעות מעקב אחר כתובות IP. מטרה זו עשויה לנבוע ממניעים כמו מעקב אחר התנגדות, אכיפת צנזורה על תוכן ועוד, כפי שמודגם בהקשר של המאמר הנוגע לאיראן, רוסיה וסין.

למרות שהיישומים הללו מבטיחים הצפנה חזקה לתוכן תקשורת, החוקרים מוכיחים שניטור תעבורת רשת מאפשר למודלים סטטיסטיים להבחין בדפוסים בזרימת הנתונים. דפוסים אלה יכולים להניב אוצר של תובנות, שעלולות לחשוף התנהגויות משתמשים ופעילויות של מפעילי מסרים מיידיים ללא ידיעתם. החוקרים חשפו שכל פעולה שמתבצעת באפליקציות הללו - בין אם זה שליחת הודעה, העלאת קובץ או פשוט הקלדה - מייצרת דפוס מובהק בזרימת נתוני התקשורת. כתוצאה מכך, תוקף יכול לאסוף מידע רב ערך על משתמשים ועל המעורבות שלהם אך ורק על ידי בדיקה ופרשנות של דפוסים אלה. החוקרים ממציאים תופעה זו כ"התקפת ניתוח תנועה".