Dry part:

הרעיון המרכזי של המאמר:

המאמר מתעסק בבעיה שקשורה לחשיפת מידע רגיש ביישומי הודעות מאובטחות כמו טלגרם וואטסאפ. הרעיון המרכזי הוא שהפעילות הקשורה לשימוש בישומים אלה, יוצרת תבניות מסוימות בזמני ההודעות ובגודל שלהן. ניתן להשתמש בתבניות אלו ולבצע ניתוח של נתוני התקשורת במטרה לזהות אנשים מסוימים, ובמיוחד את המנהלים והחברים של ערוצים ביישומים אלו.

המחקר מציע יישומים שונים של ניתוח נתוני התקשורת,כדי לזהות אנשים מסוימים בזמן אמת. הוא משתמש בשיטות סטטיסטיות להבנת התבניות המאפיינות את התקשורת, כמו זמני וגודל ההודעות. באמצעות השוואה בין התבניות של משתמשים שונים, המחקר מצליח לזהות תבניות ייחודיות שמאפיינות קבוצות של משתמשים, במיוחד מנהלי ערוצים וחבריהם.
המחקר שם דגש על השפעת משתנים שונים כמו מספר ההודעות והאופן בו הם משתמשים ביישומי הודעות מאובטחות כמו טלגרם וואטסאפ כדי לשמור על פרטיותם. הוא מביא לידי ביטוי את הקשר בין כמות המידע שנדרש לניתוח ולזיהוי מוצלח של אנשים מסוימים. בנוסף, המחקר חוקר דרכים להתמודד עם הבעיה ולהגן על הפרטיות של המשתמשים. במטרה לשפר עמידות לניתוחים של סוג זה, המחקר מציע פתרונות אפשריים, כמו הכנת רעש תקשורתי ושינויי זמני הודעות, המשפרות את הסיכוי להפריע לניתוחים ומקשות על זיהוי המשתמשים בניתוח נתוני התקשורת.

לסיכום, המאמר מציג עניין חשוב בתחום הבטחון והפרטיות בכל הקשור ליישומי הודעות מאובטחות (ווצאפ, טלגרם..). בנוסף, המאמר מספק רקע מעמיק לבעיה ומציע כיצד ניתן להתמודד עם תופעה זו ועם האתגרים הטכנולוגיים והאפשרויות הרבות הקיימות ביישומים אלה. בנוסף, המחקר שואף לעזור למשתמשים לשמור על פרטיותם ביישומים אלה ולהשיג יכולת ניתוח נתונים מוגברת ובכך לשפר את הבטחון והפרטיות של המשתמשים בישומים אלה.

כעת נתייחס למספר דברים נוספים במאמר:

1. כיצד משיג התוקף אמת קרקע על תעבורת הערוץ?

התוקף משיג אמת קרקע (זה מתייחס לנתונים אמיתיים, כמו זמני ההודעות בערוצים, הגודל של הודעות, זמני התקשורת וכו.. מציין את ההתנהגות האמיתית של המשתמשים ביישומים אלה.) על ידי הצטרפות לערוץ ה-IM היעד כחבר "קורא בלבד". התוקף צופה ומתעד את דפוסי התקשורת והתנהגויותיהם של האנשים בתוך ערוצי היעד. תהליך זה כולל איסוף נתונים על תזמון ההודעות, גדלי ההודעות וזהות המשתמשים השולחים ומקבלים הודעות. על ידי ניתוח התעבורה בשלב זה, התוקף יוצר מערך של נתונים, תמונה מדויקת של התנועה ברשת, נתוני האמת שמתקבלים מהויים בסיס של ניתוח סטטיסטי של התוקף אשר משמשים לזיהוי דפוסים ספציפיים הקשורים לתפקידים שונים בתוך הערוצים, כגון מנהלי מערכת וחברים רגילים. בשלב זה התוקף בעצם אוסף ומנתח נתונים כדי שבשלבים הבאים הוא יוכל להשתמש בנתונים על מנת לזהות אנשים בתוך ערוצי התקשורת.

2. כיצד התוקף מאזין בסתר לתעבורת הרשת?

התוקף מאזין בסתר לתעבורת הרשת תוך לכידה וניטור התקשורת בין המשתמשים ליישומי ההודעות, כמו טלגרם ו-, WhatsApp, על מנת לחשוף את תוכן ההודעות המוצפנות שנשלחות ומתקבלות בין השרת למשתמשים. תהליך זה כולל לכידת מנות הנתונים שהוחלפו בין משתמשים בזמן אמת, בזמן שהם שולחים ומקבלים הודעות בתוך ערוצי ההודעות. התהליך כולל ניתוח של הפרטים כמו הזמנים בין ההודעות (IMTs) והגודל שלהן.

על ידי לכידה וניתוח של תעבורת הרשת, התוקף מקבל גישה לנתונים המוצפנים המועברים ברשת. לאחר מכן, התוקף יכול לפעול במגוון דרכים כדי לנתח את הדפוסים והמאפיינים של התנועה, הוא מציין את התקשורת ברשת כמטריצה של זמן ואירועים, ובאמצעות השוואה בין המשתמשים השונים, הוא פועל לזהות דפוסים הקשורים לתפקידי משתמש שונים, כגון מנהלי מערכת וחברים רגילים, ולהשתמש במידע זה כדי לבצע התקפות ניתוח תעבורה.

3. תאר בקצרה את המסקנות מטבלה II במאמר.

טבלה II במאמר מציגה את התפלגות סוגי ההודעות השונים בנתוני התעבורה של הודעות מאובטחות (IM). הטבלה מספקת תובנות לגבי הספירות (count) , הנפח (volume), טווח הגדלים (size range), והגודל הממוצע (average size), של סוגי הודעות שונים, כלומר טקסט, תמונה, וידאו, קובץ ואודיו.

<u>המסקנות מטבלה II הן:</u>

1.סוגי הודעות: הטבלה חושפת את התפלגות סוגי ההודעות השונים בתקשורת ה-IM. המאמר מסווג מסרים לחמישה סוגים עיקריים, טקסט, תמונה, וידאו, קובץ ואודיו.

2. גודל ההודעה: גודל ההודעות משתנה באופן משמעותי בין סוגי הודעות שונים. כל סוג הודעה מציג טווח גדלים משלו.

3. נפח: הנפח של כל סוג הודעה, נמדד במגה-בייט, משתנה במידה ניכרת. סוגי הודעות מסוימות, למשל וידאו, בעלי נפח גדול בהרבה מהשאר.

4. גודל ממוצע: הגודל הממוצע של הודעות בין סוגי ההודעה. לדוגמה, הודעות אודיו נוטות להיות בגודל ממוצע גדול יותר בהשוואה להודעות טקסט.

טבלה II משמשת כסיכום מקיף של התפלגות סוגי ההודעות, הגדלים והתרומות של מערך תעבורת ה-IM שנאסף. מידע זה חיוני להבנת אופי התקשורת ולשלבים מאוחרים יותר של הניתוח במאמר.

4. איור 8:

תרשים 8 במאמר מציג את תוצאות הניסוי המתמקד בניתוח התנהגות המנהלים והחברים בערוץ. התרשים ממחיש את היכולת של התוקף לזהות אנשים מסוימים מתוך התנהגותם בהודעות.

כאשר המידע הנתון מכיל פרטים כמו זמן ההגעה והגודל שלהן, התוקף מסוגל לזהות מנהלים וחברים באופן מדויק ובזמן אמת. התוצאות מציינות את ההפרשים בין הקבוצות השונות, מה שמראה על הכשלונות באבטחת הפרטיות באפליקציות המידע האלו.