מסמך ייזום – KRACK ATTACK

איתי רפיעי

אלחי מנצבך

אלמוג יעקב מעטוף

הקדמה:

ברשתות אלחוטיות הAP אינו יודע את המיקום המדויק של הלקוח ומיקום הלקוח יכול להשתנות בכל רגע נתון. לכן נכון להיום, ל-AP ברשת אלחוטיות אין אפשרות לשלוח באופן אישי ללקוח את המידע שביקש. עקב כך המידע מופץ ב"אוויר" לכלל הרשת, מה שמאפשר לכל הלקוחות ברשת גישה לצפות במידע המועבר.

על מנת להגן על המידע יש לספק שכבת הצפנה (WEP) שעל גביה תעבוד הרשת. כך מי שאין לו את מפתח ההצפנה, אומנם יכול להסניף את התדר, אך לא יכול לפענח ולהבין את התוכן. החיסרון בהצפנה זו הוא שכלל הרשת מוצפנת באותו המפתח, ולכן כל לקוח עם סיסמת הרשת יכול להאזין לכלל התעבורה.

שיפור לשיטת הצפנה זו - WPA/WPA2 .

WPA משתמש בפרוטוקול, אשר מחליף את המפתח הקבוע והקטן יחסית של פרוטוקול ה-WEP ומייצר באופן דינאמי מפתח חדש לכל חבילת מידע וכך מונע התנגשויות. כמו כן, ישנן בדיקות שלמות ההודעות (כדי לקבוע אם תוקף תפס או שינה חבילות שהועברו בין הAP ללקוח).

WPA הוחלף על ידי WPA2 המשתמש בפרוטוקול הצפנה מתקדם יותר ובפרוטוקול handshake. ההצפנה מקשה מאוד על פענוח ושימוש בחבילות מידע המועברות ברשת.

חיבור WPA2 מתחיל ב-four-way handshake , שהוא תהליך המצריך החלפה של ארבע הודעות בין הAP ללקוח כדי ליצור מפתח הצפנה ולהצפין נתונים. תהליך זה מתבצע כאשר המכשיר מתחבר לראשונה לרשת. כדי להפוך את החיבורים הבאים למהירים יותר, יש לשלוח שוב רק את השלב השלישי של ה-four-way handshake . כדי לוודא שהחיבור הצליח, ניתן לחזור על שלב זה מספר פעמים. כאן נכנסת לתמונה הפגיעות ש KRACK-ATTACK מנצל.

<u>למה לתקוף רשתות אלחוטיות?</u>

בחרנו לבצע תקיפה על רשתות אלחוטיות מאחר וזוהי טכנולוגיה זמינה הנמצאת בכל מקום. ביצוע תקיפות על רשתות אלחוטיות מתאפשר די בקלות ולא דורשת אמצעים מורכבים, וניתן לבצע אותה אפילו בעזרת המחשב הביתי.

KRACK-ATTACK :

KRACK ATTACK היא התקפה המנצלת חולשה של פרוטוקול האבטחה WPA2 ברשת אלחוטית לצורך גניבת הנתונים המועברים ברשת.

התוקף יוצר העתק של הרשת האלחוטית שאליה הקורבן התחבר. כשהקורבן מנסה להתחבר שוב לרשת, התוקף מאלץ אותו להתחבר לרשת החדשה ולשלוח את אישור ההתחברות של השלב הרביעי ב-handshake אליו. לאורך כל ההתקפה, ה AP ממשיך לשלוח את השלב השלישי שוב ושוב אל הקורבן. בכל פעם שהקורבן מאפשר לחיבור לקרות, חלק מהמידע מפוענח. התוקף יכול

להשתמש במידע שאסף כדי לפענח את מפתח ההצפנה. לאחר שהצפנת ה-WPA2 נפרצה, לתוקף יש גישה למידע של הקורבן המועבר ברשת.

התקפות אלו עלולות לגרום לגניבה של מידע רגיש כמו סיסמאות, מספרי כרטיסי אשראי, צ'אטים פרטיים וכל מידע אחר שהקורבן מעביר דרך האינטרנט. ניתן להשתמש ב-KRACK גם לביצוע התקפות man in the middle attack, פיתוי הקורבן לאתר מזויף או להחדרת וירוסים דרך אתרים ברשת.

יש לציין שהתקפה זו דורשת קרבה למכשיר המותקף. התוקף והקורבן חייבים להיות שניהם בטווח של אותה רשת אלחוטית כדי לבצע את המתקפה.

למה KRACK-ATTACK?

- לא מצריכה מהתוקף יכולות עיבוד גבוהות (חומרה חזקה).
- אפקטיבית לכמעט כלל המימושים השונים של פרוטוקול זה במערכות ההפעלה השונות.
- נחשבת "אלגנטית" מאוד -אין דריסות זיכרון או בעיות במימוש תוכנתי, אלא ניצול בעיות של פרוטוקול האבטחה.
- קלה לניצול והאפקט שלה משמעותי מאוד.

יעדים לביצוע

- לפגוע בפרוטוקול "four-way handshake " בשביל השגת מפתח ההצפנה
- השגת מפתח ההצפנה.
- גישה למידע ברשת בין הלקוח לAP.

כיצד נמדדת הצלחה עבור התקפה זו?

הצלחת ההתקפה נמדדת בכך שבהתחלה הצלחנו להשיג את המפתחות הרלוונטיים בשלב ה"four-way handshake " בצורה טובה, לאחר מכן בתקיפת ה-Group Key Handshake השגנו את מפתח את GTK ובעזרת כל אלה הצלחנו להסניף את התעבורה מוצפנת של הקורבן אשר עוברת ברשת.

כיצד ניישם את המתקפה ברמת הרקע הרעיוני ביחס לטכנולוגיה הקיימת?

ע"פ רעיון ההתקפה הנ"ל נבחין בבסיס ההתקפה שהוא שליחת המפתח שוב ושוב (בשלב השלישי של ה-Four-Way Handshake) זאת על מנת ללכוד את מפתח ההצפנה החד פעמי אתו יהיה ניתן לבצע פעולת זדונית (לדוגמא, לפענח את התעבורה) בהתחשב בכך, המשאב ההכרחי הינו מתאם רשת תומך מצב מוניטור זאת מכיוון שמצב המוניטור מאפשר צפייה בתעבורת ה-Wi-Fi בערוץ מסוים מבלי להשתייך לנקודת גישה או בצורה מדויקת יותר, אנחנו מאלצים את הכרטיס רשת להעביר לנו חבילות מידע גם כאשר הוא אינו מחובר לאף רשת.

מכאן, לאחר האפשרות לצפות בתעבורה נוכל לבחור קורבן וללכוד את החבילות המיועדות (כאמור, בשלב השלישי של ה-Four-Way Handshake).
לאחר מכן, נוכל להתחקות ולבצע שליחה חוזרת של החבילות הנ"ל.
גם זאת המתאם רשת מאפשר בשימוש ספריות רלוונטיות כפי שראינו במטלה הקודמת במימוש מתקפת Evil-Twin.(נשים לב שיש כאן הכרח נוסף והוא מתאם רשת תומך מצב AP על מנת להתחקות לנקודת הגישה של הקורבן).
השליחה החוזרת תגרום לשידור נוסף של מפתח מחודש מהקורבן עם אותו PTK של שלב 2 ב--Four Way Handshake. מכיוון שהמפתח החדש נוצר על סמך אותם נתונים כמו המפתח הקודם אזי

באמצעות מניפולציות ניתן להסיק מסקנות על המפתח ואף לפצח אותו. ישנם מקרים בהם ישנה שבירה של המפתח (מכיוון שחלק מגרסאות לינוקס ואנדרואיד מאפסות את המפתח לאפס כתוצאה מהתקפה זו). כעת, ניתן להמשיך לשלב פענוח התקשורת.

נשים לב, כי WPA2 נפוצה כיום ולכן התקפה זו ניתנת לשימוש על מספר רב של פגיעים.

בעיות שעלינו לפתור במהלך הפרויקט:

נצטרך להיות במצב של MiTM מלא על מנת לשלוח את המפתח שוב ושוב אך יש לנו מק שונה (מהווה בעיה מכיוון שכבר בשלב השני שני עמדות הקצה משתמשות בכתובות המק אחת של השנייה על מנת ליצור את ה-PTK).

כמו כן, ע"פ מידע שאספנו מהאינטרנט ישנם מקרים בהם עמדות קצה מתעלמות מאותן "חבילות שלב 3" לאחר קבלת המפתחות בשלב 4 מה שיאלץ אותנו לחסום את תגובת הלקוח בצורה מסוימת ולמנוע מהנתב לקבל אותה.

תכולת העבודה והמשאבים הנדרשים לצורך ביצוע המתקפה:

חומרה:

מתאם רשת תומך מצב מוניטור על מנת לנטר את החבילות (כפי שהזכרנו לעיל) וגם מצב AP על מנת להתחקות לנקודת הגישה של הקורבן.

תוכנה:

- כל מערכת הפעלה שבאמצעותה מתאפשרת ההאזנה (מוניטור) ושליחת החבילות כדוגמת Linux
- המימוש יבוצע (בדומה למטלה הקודמת) בשפת Python כפי שהגדרנו בתחילת הקורס
- ספרית Scapy לצורך ניהול החבילות
- מכיוון שזהו מסמך ייזום בלבד תיתכן דרישה/דרישות נוספות עבור משאב/משאבים (שאינם חומרה) במהלך ביצוע הפרויקט.

כיצד ניתן להתגונן מפני התקפה זו?

קיימות כמה דרכים על מנת להתגונן מפני מתקפות אלו:

- להתקין את עדכוני התוכנה הרלוונטים של החברות השונות. החולשה עצמה נמצאת במימוש של supplicant_wpa ולא בשכבות הגבוהות יותר ולכן אין כאן איזה הגדרה לשנות או לערוך.
- ניתן להשתמש בVPN (מומלץ לבדוק את ספקי השירות), חיבור מאובטח המאפשר לשלוח ולקבל מידע מהאינטרנט בצורה בטוחה בעזרת הוספת שכבות הגנה לפאקטות שנשלחות.
- שימוש בחיבור קווי (Ethernet) לנתב / נתונים סלולרים.
- ניתן להתקין HTTPS Everywhere שבמידה אתר אינטרנט מציע גם HTTP וגם HTTPS הוא יעדיף את הHTTPS (אך במידה וקיים רק גישה לא מוצפנת HTTP תוסף זה לא יוכל לעשות דבר)

מקורות:

- https://he.wikipedia.org/wiki/WPA
- https://www.cloudflare.com/learning/security/what-is-a-krack-attack/
- https://techcrunch.com/2017/10/16/heres-what-you-can-do-to-protect-yourself-from-the-krack-wifi-vulnerability/
- https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn