**המחלקה להנדסת תוכנה**

**פרויקט גמר תשע"ז**

**אבטחת נתבים ברשת בייתית**

**Securing wireless networks for home routers**

**ליאור ספיר liorsap1@gmail.com**

**יועד שירן shooki@gmail.com**

**מנחה אקדמי: ד'ר אללוף מרים.**

**אישור: תאריך:**

**רכזי הפרוייקטים: ד'ר אללוף מרים ו-ד'ר יגל ראובן.**

**אישור: תאריך:**

|  |  |  |
| --- | --- | --- |
| **#** | **מערכת** |  |
| **1** | **מאגר קוד** | **https://github.com/sh00ki/JCE-Project** |
| **2** | **יומן** | **https://trello.com/b/Ter3qxak/yoad-lior-project** |
| **3** | **ניהול פרוייקטים** | **Github** |

**1. מבוא**

היום, השימוש ברשתות אלחוטיות (WIFI) הופך להיות כל כך שכיח, יש צורך בנקיטת אמצי הגנה ואבטחה על הרשתות האלחוטיות. מעצם טיבעה, תקשורת אלחוטית מתאפיינת בכך שהמידע המשודר מהמחשב ואליו חשוף להאזנה. באמצעות כלים פשוטים, ניתן להאזין לתשדורת האלחוטית, מה שעלול להביא לחשיפה של מידע רגיש ומקורות שאין אנו רוצים לחשוף בפני אחרים.

בנוסף על כך, רשת אלחוטית בייתית או משרדית שאינה מאובטחת כיאות לעולם הגדול, חושפת את הנתב ומשתמשי הרשת הביתית עצמה, להאקרים וגורמים זרים המעוניינים לזרוע בה הרס, לגזול רוחב פס ולדלות אינפורמציה רגישה מבלי שמשתמשי הרשת ידעו על כך.

על מנת לפרוץ לנתב האלחוטי ולרשת הביתית, כל מה שנדרש הוא מחשב נייד, תוכנה וקצת סבלנות. לכן יש צורך חיוני ליישם מנגנוני אבטחה שיגנו על הרשת האלחוטית.

ברצוננו להדגיש כי אין אבטחה ברמה מושלמת לשום רשת אלחוטית. פורץ או גורם זר עיקש וחדור מטרה ברורה, עם אמצעים להשגתה, יוכל להתגבר על כל מנגנון אבטחה שניישם במהלך הפרויקט. עם זאת ובהנחה שעל המחשבים לא שמורים סודות ביותר, יישום האבטחה שנציג בפרויקט, יגביר את בטחון הרשת האלחוטית בבית ובמשרדים קטנים.

**תיאור הבעיה:**

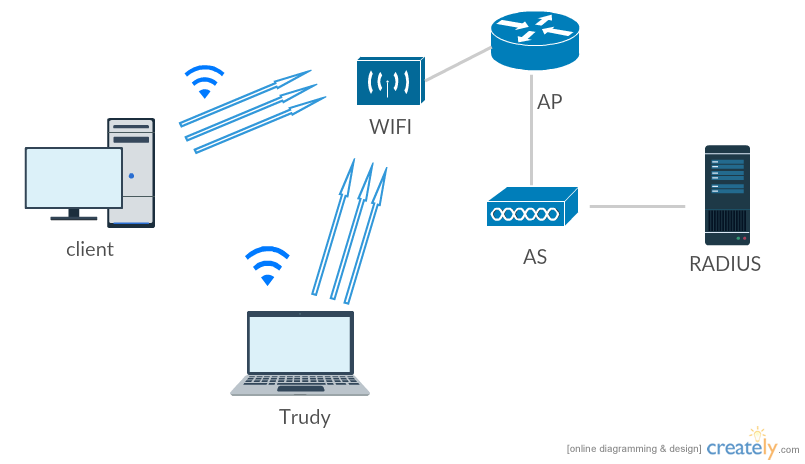
- היום, בעידן בו כולנו שומרים מידע רגיש על מחשבינו הביתיים ומשתמשים בשירותים הנזקקים לרשת אינטרנטית, מאוד קל לצוטט, להאזין ולדגום את המידע של תעבורת תשדורת האינטרנט ע"י האזנה לרשתות שמבוססות WIFI. ישנם כלים רבים חינמים, שניתן בעזרתם לפצח את תהליך האימות ולפצח את סיסמת הכניסה לרשת האלחוטית.

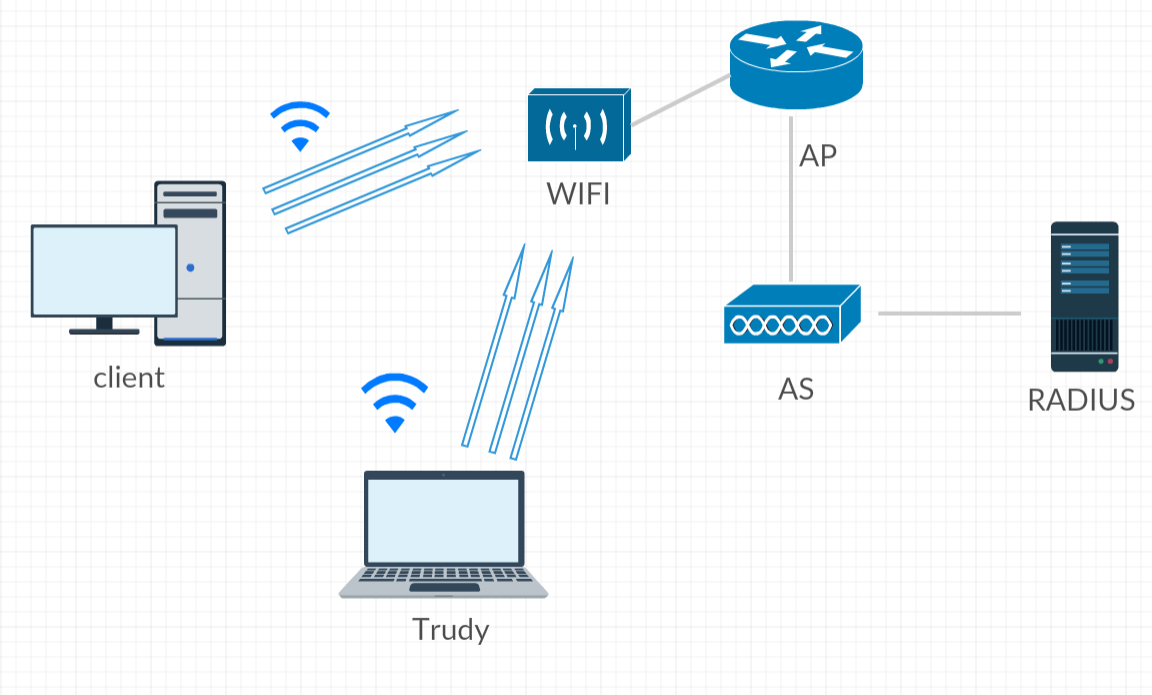
(למשל ע"י הכלי Aircrack-ng וכלים נוספים שנפרט עליהם בהמשך המסמך).

- בפרויקט שלנו נתמקד ב: פתרון הבעיה של האזנה ודגימה של תהליך האימות לצורך כניסה לרשת הWIFI ברשתות בייתיות ומשרדיות כחלק ממתקפת Brute force ו-נציע פתרון ישומי להגנה, שעליו חשבנו (נציג אותו בהמשך המסמך.

בעת דגימה של תהליך האימות (4-way-handshake) ע"י גורם שלישי (האקר או כל גורם זר אחר), המידע המכיל נתונים על הכניסה לרשת האלחוטית חשוף, מה שנשאר זה רק לפצח את אימות הכניסה בעזרת מילון סיסמאות. כל מה שנשאר להאקר, זה להריץ קובץ אשר מכיל אוסף סיסמאות רחב, ללא ידיעה של הנתב\המשתמש על הנעשה מצד הפורץ בכדי לפצח את סיסמת האימות בכדי לקבל כניסה לרשת הביתית אלחוטית.

מתקפה זאת נקראת Brute Force על רשתות שמבוססות WIFI לצורך דגימה של תשדורת הרשת, מתבצעות בשכיחות גבוהה. אחת מהדרכים לבצע מתקפה שכזו, היא בדרך הזו: ה supplicant  (client) שולח בקשה להתחברות לAuthenticator (router) ומתחיל תהליך אימות שמתרחש ברשת. כיו"ם האימות אינו מתבצע בנתב ולכן ניתן להאזין לתהליך האימות דרך הרשת. לדגום את המידע של האימות (לדגום את המפתח של הPreshared Key של הרשת WIFI  ולהיכנס לתוך הרשת, לצפות במחשבים נוספים, האזנה MITM וסוגים שונים של מתקפות)



****