BYOD Vulnerabilities by rogue AP

עזריאלי -

המכללה האקדמית להנדסה ירושלים

המחלקה להנדסת תוכנה

מגישים:

שם	דור הראל	יועד שירן	אלון שמילוביץ
ת.ז	300300563	302978713	34616359
כתובת מייל	dor1harel@gmail.com	shooki@gmail.com	alonshmilo@gmail.com
טלפון	054-4710936	058-4888848	050-9769095

מטרת הפרויקט:

מטרת הפרויקט הינה ניצול פגיעות השיטה של BYOD – Bring Your Own Device על ידי הקמה של Rogue Access Point ויצירת גשר שמטרתו לגרום למשתמשים ברשת האלחוטית "לעבור" דרכנו ובכך לנטר את החבילות שנשלחות ועוד.

שיטת BYOD – Bring Your Own Device:

בעידן שלכל אדם יש מכשירי תקשורת שונים: כמו סמארטפון, לפטופ, טאבלט, שעון חכם וכו', וגם ככל שרעיון ה- IOT – Internet Of Things מתפתח ותופס תאוצה בחיי היום יום שלנו, נוצר מצב של פגיעות גדולה של ארגונים גדולים שמעסיקים עובדים על ידי כך שמתבצע שימוש במכשירים אלו לצרכי עבודה, ללא יכולת של הארגון לפקח את רמת האבטחה בצורה המתאימה לו. למשל – בצה"ל מבצעים בכירים במערכת שימוש במכשירים סלולריים פרטיים, דבר היכול להוות סיכון בטחוני עצום בכל הקשור לביטחון המידע ודליפת מידע. בעבר, היה שימוש רק במכשירים צהליים מוצפנים והמעבר הזה למכשירים פרטיים חכמים, עלול להוות מכשול לצה"ל בפרט ולביטחון המדינה בכלל. נסקור את הסיכויים והסיכונים של השיטה.

סיכויים:

1. העלאת פונקציונליות של העובד – כל עובד משתמש בפלטפורמה שנוחה לו, שהוא מכיר, ולכן ישנו שיפור בזמינות שלו, באפקטיביות ובמורל.
2. המידע זמין יותר עבור העובד, גם אם אינו נמצא במקום העבודה או ליד מחשב.
3. מאפשר גמישות בעבודה – ניתן לעבוד מעוד מקומות מלבד במשרד. לדוגמא – הורים עובדים יכולים להישאר בבית עם ילד חולה ועדיין לעבוד.

סיכונים:

1. בעיית גניבות – עלולה להיווצר בעיה של גניבת מכשירים עם מידע רגיש. למשל – בעבר כבר נגנב לפטופ מרכבו של קצין צה"ל בדרגה גבוהה.
2. וירוסים וחולשות – סיכון שעובד ייחשף לוירוסים וחולשות בשל שימוש פרטי במכשיר.
3. העובד עלול שלא להתקין עדכוני אבטחה חשובים או לחילופין להשתמש בעדכוני תוכנה שלא נבדקו כראוי למידע הרגיש ובכלל – שיגרמו לקריסה של מחשב.
4. בעיות תאימות – מכשירים שונים, מערכות הפעלה שונות, תוכנות שונות שמריצות את אותם הקבצים. כמו למשל Word של Microsoft לעומת Pages של Mac iOS.
5. ואחת הבעיות הגדולות – המכשיר יכול להפרץ על ידי האקרים בשל חוסר זהירות של העובדים. העובד בעצמו יכול לפרוץ את המכשיר כדי להיחשף למידע ולתוכנות שאולי הארגון לא מאפשר.

ניתן לחלק ל4 סוגים את גישת הארגונים כלפי BYOD:

1. HYOD – Here is You Own Device – המכשירים מסופקים על ידי הארגון, ובכך הארגון מפקח על רמת האבטחה, הקונפיגורציה של המכשירים, המגבלות שלו וכו'.
2. CYOD – Choose You Own Device – הארגון מספק מספר של מכשירים מתוכם העובד יכול לבחור את המכשיר. הגישה אינה שונה בהרבה מגישה 1, אך ההבדל הוא שהמשתמש יכול להתקין אפליקציות ותוכנות מסויימות לרוב דרך חנות אפליקציות של הארגון.
3. BYOD – Bring Your Own Device – העובד בוחר את המכשיר איתו הוא עובד, ורוכש אותו בעזרת הארגון עצמו. המשתמש יכול לבחור את האפליקציות והתוכנות שירוצו על המכשיר. גישה זו הינה פגיעה בשל חוסר יכולת של הארגון לפקח על רמת האבטחה במכשיר והתוכן המצוי עליו, בעיקר בארגונים גדולים בהם יש אלפי מכשירים. הדבר היחיד שהארגון יכול לעשות הוא לקבוע מדיניות שימוש במכשירי תקשורת, אך קיים קושי רב לאכוף הנחיות אלו באופן מלא ולמנוע בעיות אבטחת מידע.

4. OYOD – On Your Own Device – המשתמש יכול להביא איזה מכשיר שיחפוץ בו, ללא תמיכה של הארגון כלל. האחריות לניהול המכשיר חלה על המשתמש בלבד ואין אף מדיניות שנקבעת על ידי הארגון. זוהי הגישה הפגיעה ביותר בשל חוסר התערבות מוחלט מצד הארגון במכשירי התקשורת.

כלים

הכלים בהם השתמשנו במהלך העבודה הינם:

1. כרטיס רשת חיצוני wifisky בעוצמה גבוהה.
2. אנטנה כיוונית לצורך מדידות.
3. מחשב נייד עם מערכת הפעלה kali linux, עליו הותקנו תוכנות יעודיות.
4. מחשבים ניידים שונים.
5. תוכנת WireShark.
6. אתר למדידת מהירויות.
7. אפלקציית מדידת עוצמה - wifi-analyzer.
8. נתב המשמש כ-repeater לצורך יצירת נקודת AP.

בפרוייקט זה בעצם נקים Evil twin Rogue Access Point שיהווה עבור המשתמשים ברשת bridge שדרכו אנו נוכל לנטר את כל תוכן התעבורה ברשת מבלי שהמשתמשים ידעו על כך.

נבדוק את ההשפעות של חיבור Access Point שכזה מבחינת מהירויות שונות, זיהוי הAccess Point המתחזה, ניתוב במסלולי תקשורת והשפעת עוצמת השידור והתיעדוף לאיזה Access Point להתחבר.

כתבנו סקריפט שמבצע:

1. מאתחל את כל הנתונים לפני הביצוע.
2. מבצע התקנות של כלים נדרשים לצורך הקמת נקודת הגישה.
3. שואל מה הMAC Adress שברצוננו לשדר, כאן נבחר באותה הכתובת של הרשת האלחוטית במקום, על מנת שיתחברו אלינו.
4. שואל על איזה ממשק אנו מעוניינים להקים את נקודת הגישה.
5. שואל איזה שם להעניק לנקודת הגישה. כאן נבחר באותו השם של הרשת האלחוטית במקום, על מנת שלא יזהו את הרשת המתחזה.
6. שואל באיזה ערוץ אנו מעוניינים לשדר.

7. שואל איזה ממשק אנו מעוניינים שיהווה את הגשר לרשת האינטרנט.
8. מקים שרת DHCP לשם חלוקת כתובות IP.

הסקריפט שלנו בונה טבלאות חוקים לIP Tables לניתוב ומקים DHCP server לחלוקת כתובות הIP שאנחנו נחלק מתחתינו, מעביר את הממשק למצב monitor, והוא משדר על ידי כלי שנקרא airbase את כל הנתונים שברצוננו לחשוף.

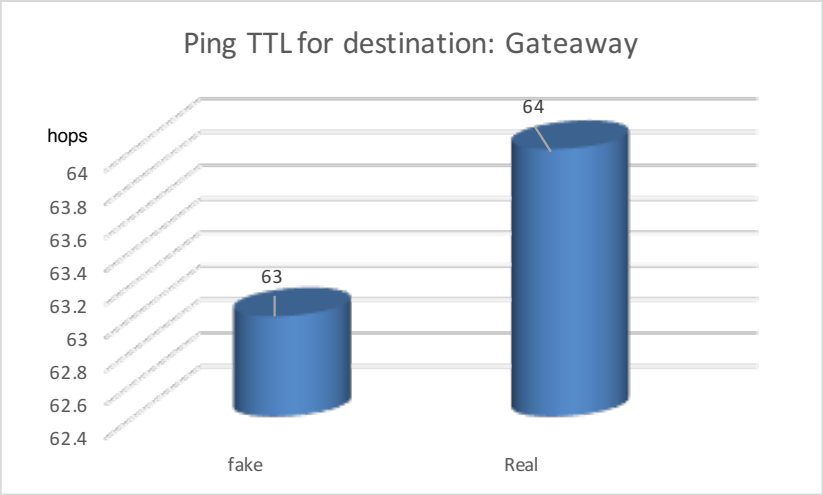
ה-airbase יוצר ממשק וירטואלי (AT0) שמורכב על המוניטור שיצרנו לפני (wlan<#>mon, השם של המוניטור יכול להשתנות ממחשב למחשב), ומחבר אליו את הקונפיגורציה של הDHCP, ומבצע את חלוקת הכתובות.

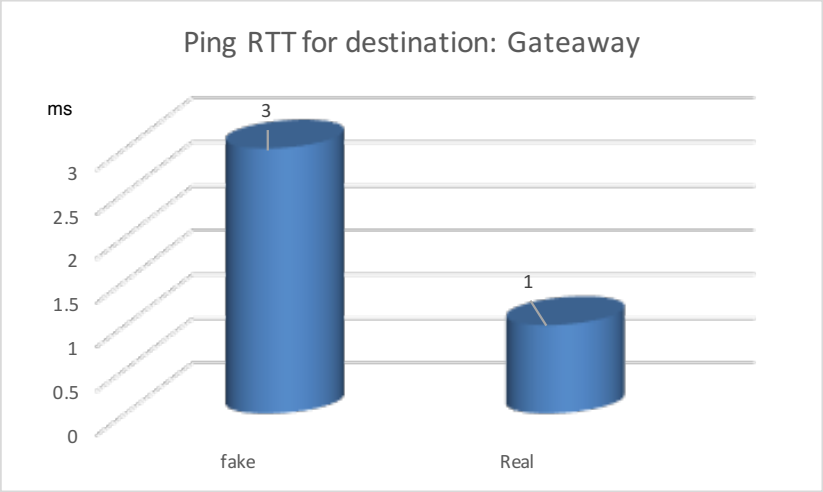
<u>מדידות שיבוצעו</u>

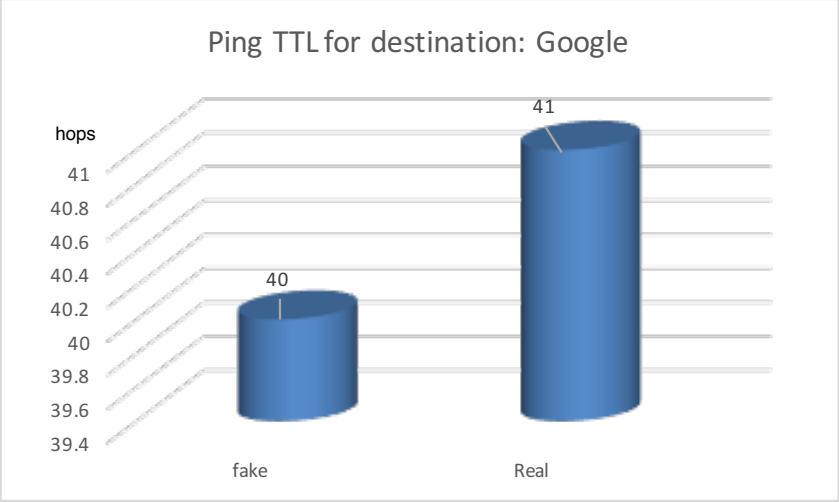
1. האטה של האינטרנט:
   - על ידי Ping.
   - על ידי Traceroute – האם הוארך המסלול.
   - בדיקת מהירות: העלאה, הורדה ו-Ping.
2. מדידת עוצמת שידור:
   - fake AP מול נתב רגיל המחובר לאינטרנט.
   - העדפת חיבור של fake AP מול נתב רגיל.

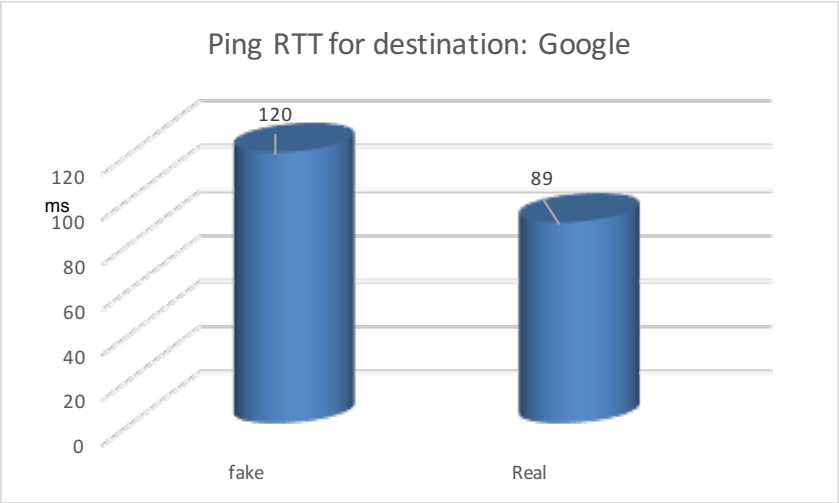
תוצאות:

ביצוע פינג עם הFake AP וללא. מיקום: בית פרטי









הסבר התוצאות:

בביצוע Ping ללא הAccess Point המתחזה, הגענו לתוצאה של TTL מסויימת וכאשר חיברנו את הAccess Point הגענו לתוצאה הגדולה ב-1 מהתוצאה הקודמת. מכאן, שהצלחנו לחבר את הAccess Point בצורה נכונה ושהמחשב זיהה את הAccess Point המתחזה וביצע ניתוב דרכו.

בנוסף, מעבר דרך הראוטר המתחזה, יכול בהחלט להסביר את זמן הRTT הגדול יותר, זאת ניתן לראות בגרפים של הRTT.

ביצוע Traceroute לגוגל, עם ה-fake Access Point וללא

IP	Real			Average	Fake			Average
10.0.0.254					3	2	3	2.67
192.168.1.1	1	1	3	1.67	3	3	6	4.00
10.133.160.1	10	9	9	9.33	10	13	10	11.00
212.199.24.218	13	13	16	14.00	16	16	16	16.00
212.199.24.217	13	16	11	13.33	15	14	15	14.67
212.199.5.62	13	16	12	13.67	16	14	20	16.67
212.199.5.113	12	12	12	12.00	16	21	16	17.67
80.179.166.134	73	71	71	71.67	72	73	72	72.33
72.14.216.121	71	71	73	71.67	72	72	73	72.33
216.239.58.184	71	72	76	73.00	134	76	75	95.00
216.239.57.143	71	71	75	72.33	74	75	75	74.67
108.170.232.77	75	78	129	94.00	77	80	78	78.33
74.125.37.97	90	86	86	87.33	89	91	88	89.33
216.239.42.98	86	88	86	86.67	87	88	90	88.33
Request timed out.	*	*	*	*	*	*	*	*
8.8.8.8	86	85	86	85.67	89	113	113	105.00

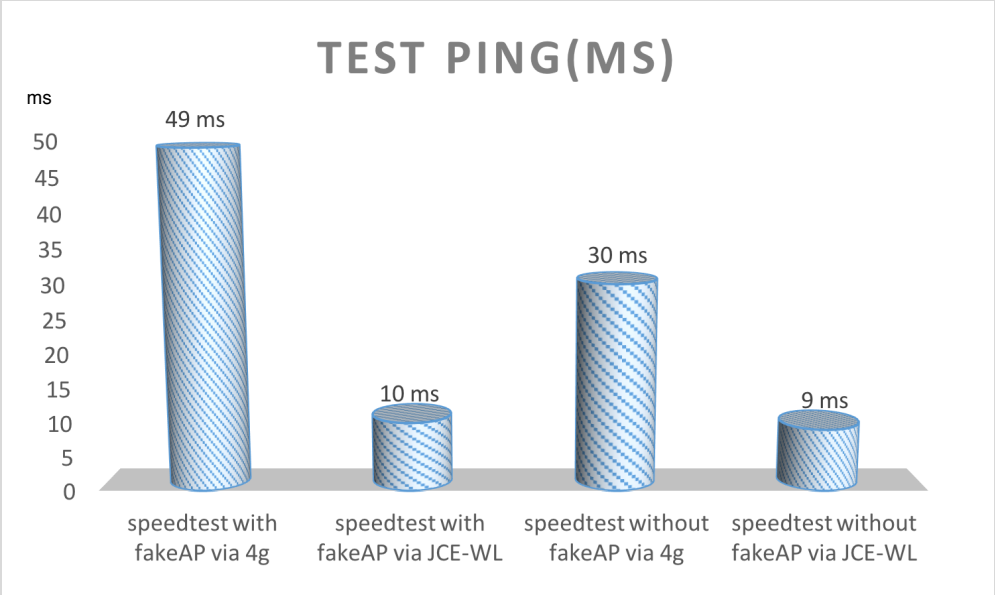
הסבר התוצאות:

בטבלה זו ריכזנו שני ביצועי Traceroute- האחד כאשר הAccess Point המתחזה מחובר, ואחד ללא. ניתן לראות שכאשר הAccess Point המתחזה מחובר, רשימת הנתבים גדולה ב-1 מאשר ללא.

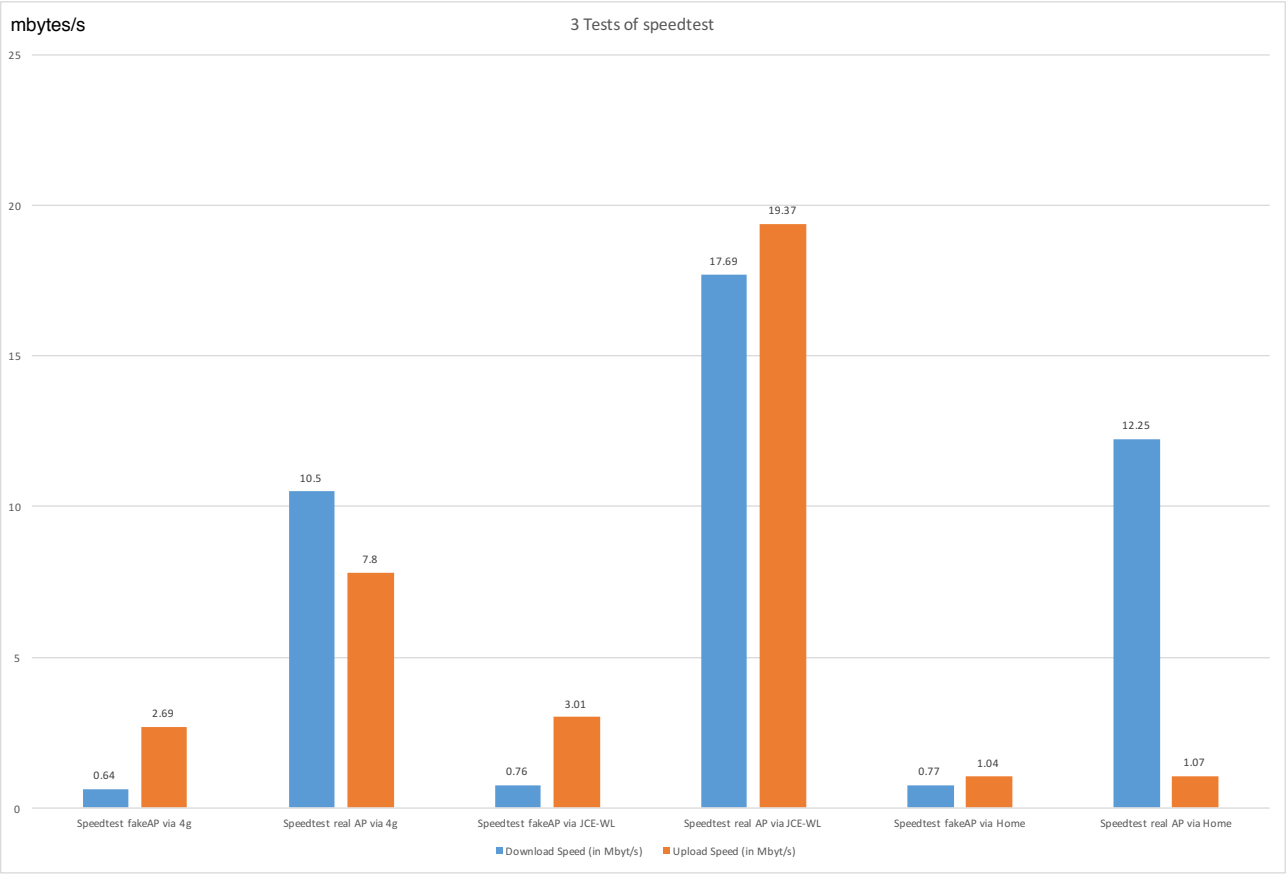
בנוסף, ציינו היכן ממוצע הזמנים גדול יותר (מסומן בירוק) - וראינו שכאשר הAccess Point המתחזה מחובר, הזמנים הממוצעים גדולים יותר, מה שהגיוני, בשל העובדה שמתווסף הזמן של הAccess Point המתחזה, פחות או יותר. ניתן גם לראות שהתוספת בכל שורה היא בערך בזמן של הAccess Point המתחזה לפי השורה הראשונה - 2.67.

אנו רואים שבנתב 108.170.232.77 ישנו היפוך של זמנים, וזאת עקב חבילה אחת ספציפית שהתעכבה מתוך ה-3, משום שאנו רואים שבשתיים מהחבילות - הגענו לערכים נורמליים.

ביצוע בדיקת מהירות עם הFake AP וללא, כאשר בודקים מול הרשת של המכללה ומול רשת סלולרית.



ביצוע בדיקת העלאה והורדה ב3 אפשרויות רשת שונות



הסבר התוצאות:

ניתן לראות ירידה משמעותית בקצב ההורדה. זאת ניתן להסביר על ידי כך שיש עוד נתב שמאט את הקצב. הנתב שלנו הינו נתב תוכנתי ולא חומרתי ולכן הניתוב מתבצע באופן איטי יותר. בנוסף בנתב הרגיל ישנם אלגוריתמים של תיעדוף חבילות, מה שאצלנו אין, ולכן הנתב פשוט מעביר את החבילות ללא ביצוע חישובי כדאיות והעדפה שיעזרו לו בהורדה מהירה יותר.

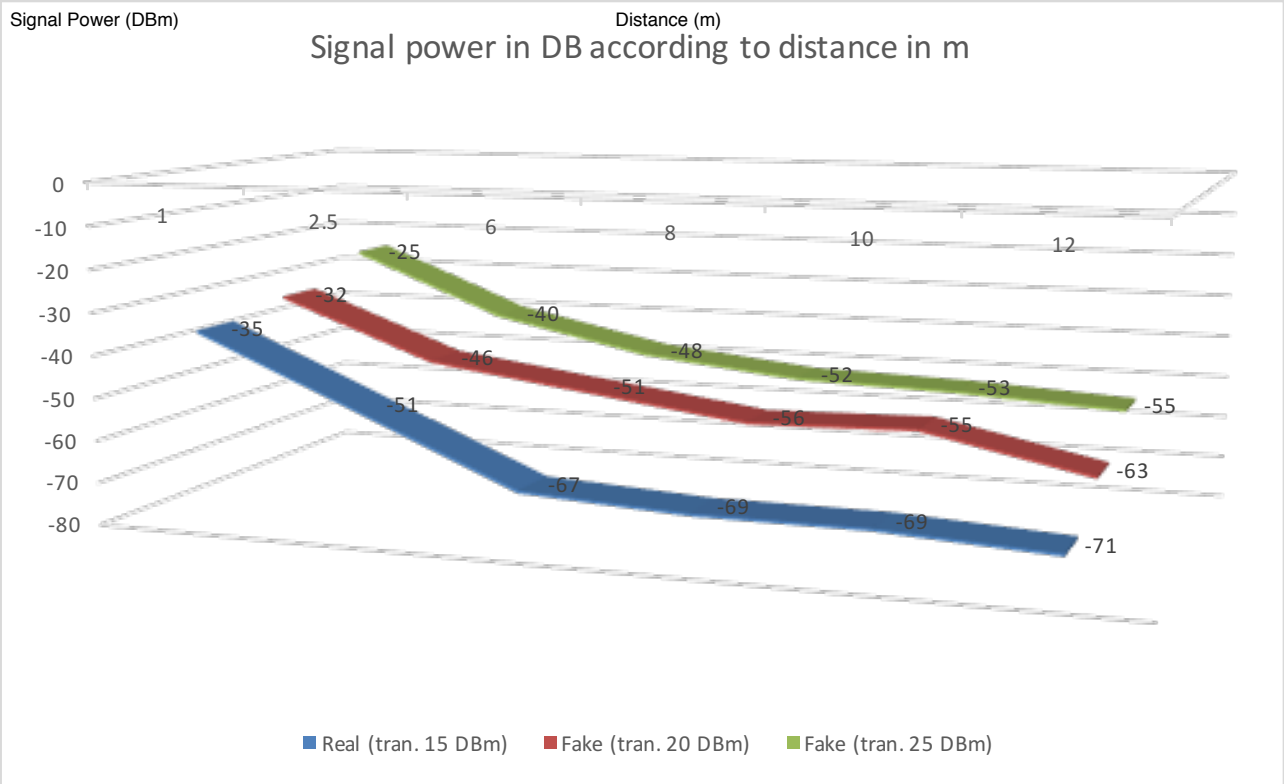
העלאה לעיתים אצלנו יותר מהירה מאשר ההורדה משום שאין לנתב צורך לדעת להיכן הוא מעלה אלא פשוט מבצע את ההעלאה.

מדידת עוצמת שידור והעדפה:

הסבר התוצאות:

ככל שהמרחק גדול יותר, הקליטה יורדת בצורה די לינארית כמצופה. עוצמת האות גדלה ככל שמגבירים את עוצמת השידור. ועוצמת האות תהיה גדולה יותר ככל שמתקרבים למקור השידור.

ביצענו את הבדיקות משני מחשבים ניידים ובשתי מערכות הפעלה שונות ותמיד ההעדפה הייתה להתחבר לנקודת הגישה המזוייפת, משום שהאות הייתה חזקה יותר.



מסקנות הפרויקט:

במהלך הפרוייקט ביצענו בדיקות ומדידות תוך שימוש בנקודת גישה מזוייפת, על מנת ללמוד את הסיכונים כאשר מתבצע שימוש במכשירי תקשורת שונים שלא נמצאים ברמת אבטחה מספקת וברשתות שמחוץ למקום העבודה ובתחומה, בהם יכול להתקיים מצב של נקודות גישה מזוייפות המיועדות לגניבת מידע ללא ידיעת המשתמש.

מצאנו ש:

1. כשנשדר בעוצמת שידור חזקה יותר על אותו כתובת mac, באותו הערוץ והשם יהיה זהה, תהיה העדפה של משתמשים להתחבר לאות יותר חזק, כלומר לנקודת הגישה המזויפת. וזאת משום שהוא משדר בצורה יותר חזקה.

2. כשנשדר על אותה הכתובת mac, אותו ערוץ ואותו שם, אנו נראה רק רשת אחת. כלומרף המחשב לא יידע להבדיל בין הרשת המזוייפת והרשת האמיתית, והתחברות בעצם תהיה לרשת המזויפת - זו מטרתנו.

3. היצירה של הAP הוא בעצם גנרי - כאשר משתמשים בנתונים הנדרשים הבאים: כתובת mac, ערוץ ושם, יכולים לחקות כל רשת קיימת, בכל מקום שהוא. וזהו בעצם הגשר - הbridge שאנו יוצרים לרשת האמיתית.

4. בצורה זאת, ניתן גם לבצע הגדלה של טווח הקליטה של הרשת על ידי עקיפה של פרוטוקול WPS (על אותו רעיון של הwifi באמסטרדם).

5. כשהעוצמות השידור כמעט זהות נוצר מצב של בלבול - המכשיר אינו יודע לאיזו רשת להתחבר, מבצע קפיצות בין שניהם, דבר היוצר ניתוקים תכופים.

6. לא כל כרטיס רשת יכול לבצע פעולה זו - ישנם כרטיסי רשת שאינם תומכים בשתי הפעולות במקביל - קליטה ושידור.

7. התחברות אוטומטית תתרחש רק כאשר יתבצע שימוש באותו פרוטוקול האבטחה שהיה בשימוש קודם לכן.

8. לא ניתן לשנות כתובת mac על ידי תוכנה. כתובת זו צרובה בחומרה. בפועל, לא שינינו אותה, אלא רק בצורה תוכנתית.

9. כיצד משתמש יודע שהוא מחובר לנקודת גישה מזוייפת? משתמש מתחיל יבצע בדיקה לIP שלו, יבצע traceroute ויבדוק את שם הנתב. משתמש מתקדם יבצע בדיקת ערוץ, בדיקת כתובת mac ויבדוק את מהירות הגלישה. ומשתמש מומחה יבצע בדיקה של שעון clock skew בשיטת הleast square fitting.

מסקנות אלו חושפות את פגיעות השיטה של BYOD בעיקר בצד המשתמשים, ומדוע תאגידים נזהרים בשימוש בעקרונות מנחים אלו. דבר זה יכול ליצור בעיית אבטחת מידע גדולה, בעיקר בארגונים בעלי מידע רגיש כמו צבא, תעשיות בטחוניות, אך לא רק - גם בחברות פרטיות המעוניינות לשמור על עצמן מפני ריגול תעשייתי, לשמור על המקוריות והחדשנות שלהן.

מצאנו שBYOD פגיע על ידי כלים בסיסיים קלים להשגה. ויש לנקוט בצעדים מונעים, ומלכתחילה לשקול את השימוש בגישות אלו בהתאם לרמת הסודיות והאבטחה הנדרשים, תוך כדי ניצול היתרונות של גישה זו.

ספרויות ואתרים רלוונטיים:

http://www.juniper.net/techpubs/en_US/junos-space-apps/network-director2.0/topics/concept/wireless-rogue-ap.html

http://www.rogueap.com

http://ccm.net/contents/805-risks-related-to-wireless-wifi-networks-802-11-or-wi-fi

http://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1191&context=etd_projects

www.speedtest.net